Vilniaus Universitetas
TARPTAUTINIŲ SANTYKIŲ IR POLITIKOS MOKSLŲ INSTITUTAS

TARPTAUTINIAI SANTYKIAI IR DIPLOMATIJA
MAGISTRO PROGRAMA

JUSTĖ TYLAITĖ
II kurso studentė

Atsakomybės priskyrimas valstybei kibernetiniuose konfliktuose: nuo teorijos link taikytinos praktikos

MAGISTRO DARBAS

Darbo vadovas: Prof. Tomas Janeliūnas

Vilnius
2017m. gegužės 15 d.

MAGISTRO DARBO PRIEŠLAPIS

Magistro darbo vadovo išvados dėl darbo gynimo:

.....

.....

.....

.....

..... **.....** **.....**

(data) (v., pavardė) (parašas)

Magistro darbas įteiktas gynimo komisijai:

..... **.....**

(data) (Gynimo komisijos sekretorės parašas)

Magistro darbo recenzentas:

.....

(v., pavardė)

Bakalauro/magistro darbų gynimo komisijos įvertinimas:

.....

Komisijos pirmininkas:

Komisijos nariai:

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ

Patvirtinu, kad įteikiamas darbas „Atsakomybės priskyrimas valstybei kibernetiniuose konfliktuose: nuo teorijos link taikytinos praktikos“ yra:

1. Atliktas mano pačios ir nėra pateiktas kitam kursui šiame ar ankstesniuose semestruose;
2. Nebuvo naudotas kitame Institute/Universitete Lietuvoje ir užsienyje;
3. Nenaudoja šaltinių, kurie nėra nurodyti darbe, ir pateikia visą panaudotos literatūros sąrašą.

Justė Tylaitė

BIBLIOGRAFINIO APRAŠO LAPAS

Tylaitė J. Atsakomybės priskyrimas valstybei kibernetiniuose konfliktuose: nuo teorijos link taikytinos praktikos, magistro darbas / VU Tarptautinių santykių ir politikos mokslų institutas; darbo vadovas T.Janeliūnas – V., 2017. – 53 p.

Reikšminiai žodžiai: kibernetinė erdvė, atsakomybės priskyrimas, suverenitetas, teisinė atsakomybė, valstybės atsakomybė, valstybės įsitraukimas.

Šiame darbe nagrinėjamas egzistuojančios tarptautinės teisės pritaikomumas, siekiant priskirti atsakomybę už kibernetinėje erdvėje vykstančias atakas valstybėms. Atsakomybės priskyrimas yra vienas esminių elementų, siekiant užtikrinti tarptautinį saugumą. Valstybės įsitraukimo planuojant, organizuojant ar vykdant atakas tiesiogiai, ar per nevyriausybinius veikėjus nustatymas gali padėti priskirti atsakomybę valstybei ir įgalinti teisinę atskaitomybę arba atsaką dėl neteisėtų kibernetinėje erdvėje vykstančių veiksmų.

Pateikiama teisinės bazės, taikytinos konfliktams kibernetinėje erdvėje apžvalga. Siekiant nustatyti ar valstybės atsakomybės priskyrimas įmanomas, atvejo analizei taikomas Jason Healey valstybės įsitraukimo spektras. Precedentų analizei pasirinktas 2006-2013 m. JAV karinio ir gynybos sektoriaus šnipinėjimas, kuris, remiantis tyrimo medžiagos įrodymais, priskiriamas Kinijos vyriausybei.

Turinys

Įvadas

Kartu su sparčia technologine pažanga į nacionalinių valstybių ir tarptautinę darbotvarkę patenka ir naujos grėsmės. Kibernetinio saugumo klausimai, nors ir ne visada šiuo pavadinimu, į saugumo darbotvarkę įtraukti jau paskutiniuosius tris dešimtmečius. Išsiplėtė kibernetinių grėsmių formos, pradedant nuo kompiuterinių virusų ir kitų kenkėjiškų programų, iki nusikaltimų kibernetinėje erdvėje, kibernetinio terorizmo ir kibernetinio karo. Taip pat kito ir kibernetikos panaudojimo galimybės[1].

Per daugiau nei 20 metų asmenų, aktyviai naudojančiu internetą, skaičius ženkliai išaugo, apie 40% žmonijos turi priėjimą prie interneto[2], taigi valstybės, nevyriausybiniai veikėjai, verslas ir individai tampa tarpusavyje glaudžiai susiję, vieni nuo kitų priklausomi kaip niekada anksčiau. Šalia tradicinių sausumos, oro, jūrų ir kosmoso erdvių paraleliai iš lėto išaugo ir "penktosios erdvės" - kompiuterinių tinklų ir sistemų - integravimas į karinį sektorių.[3] Kibernetikos specifika, t.y. neapibrėžtumas ir anonimiškumas, o taip pat keblumai taikant tarptautinės teisės normas kibernetinėje erdvėje vykstantiems veiksmas vertinti, didina kibernetinių nusikaltimų ir išpuolių "patrauklumą". Tuo pačiu auga ir tikimybė, kad kibernetinėmis atakomis bus imta naudotis ne tik kaip "švelniosiomis priemonėmis" (pvz. šalia propagandos), bet ir kare, be realios teisinės atsakomybės už įvykdytus išpuolius.

Stebint pastarojo dešimtmečio įvykius tampa aišku, jog kuo labiau technologiškai pažangi valstybė, tuo didesnė tikimybė, kad ji gali tapti kibernetinių atakų taikiniu. Grėsmės šaltinis gali kilti tiek iš pavienių programišių, tiek iš ideologinių motyvų turinčių asmenų ("hacktivists"), valstybių ar kriminalinių ir teroristinių organizacijų. Geografinis atstumas ir sienos nebeturi reikšmės, nyksta laiko perspektyva.

Problema: Nors kibernetiniai išpuoliai tampa vis didesne nacionalinio saugumo problema, valstybės iki šiol nesugeba rasti tinkamų mechanizmų, kaip apibrėžti atsakomybę už išpuolius valstybiniu lygiu, net jei nuo to, kas tampa atsakingas už įvykdytus išpuolius, gali priklausyti atsako į kibernetines grėsmes efektyvumas.

Akademikų akiratyje diskusijos kibernetikos tema suaktyvėjo po 9/11 įvykių, augant kibernetinių atakų skaičiui ir vis labiau stiprėjant poreikiui rasti sutarimą dėl atsakomybės už

[1] Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. London: Routledge, 2008.
[2] Internet Users, Internet Live Stats <http://www.internetlivestats.com/internet-users/> [Žiūrėta 2017 03 09]
[3] Nils Melzer, "Cyberwarfare and International Law", UNIDIR, 2011, 3. <http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>

kibernetinėje erdvėje įvykdytas atakas priskyrimo. Valstybės atsakomybė yra neabejotinai vienas svarbiausių elementų siekiant užtikrinti tarptautinį saugumą.[4] Vis dėlto daugelis akademikų pirmiausiai skiria dėmesį nevyriausybiniams veikėjams ir kibernetiniam terorizmui[5], dažniausiai ignoruodami valstybės atsakomybės priskyrimo ir suvereniteto klausimus. Netgi augantis susidomėjimas interneto teise ir informacijos bendruomenėmis neįtraukia valstybės atsakomybės klausimo kaip prioriteto.[6] Priskyrimo problemai vis labiau judant prie kritinės ribos, dažnėjant kibernetinėms atakoms prieš konkrečias valstybes su aiškiai numanomu tikslu sukelti žalą, dauguma išpuolių taip ir lieka neidentifikuoti, nes neatitinka taip vadinamojo „pakankamumo kriterijaus“, kurį suformulavo M.N.Schmittas,[7] t.y. įrodymų trūkumo atakai priskirti.

Ilgą laiką buvo dvejojama, ar kibernetinės atakos priskyrimas galimas, kai “įtariamųjų laukas” apima ne tiek dažnai valstybes, kiek pavienius asmenis ar organizacijas, veikiančias valstybės teritorijoje. Pastarojo dešimtmečio diskusijose, po nesėkmingų bandymų apibrėžti kas kaltas ir turi priimti atsakomybę už kibernetines atakas, pastebima nauja srovė. Remiantis prielaida, jog būtent nacionalinės valstybės, o ne individai, turi būti laikomos atsakingomis už kenkėjiškus veiksmus ir kitoms valstybėms bei jų sistemoms sukeltas grėsmes[8], kibernetinės atsakomybės diskusijos perkeliamos į kitą lygmenį. Ekspertai ir politikos formuotojai pasiūlė idėją, kurią išplėtojo Jason Healey, siūlydamas laikytis atsakomybės priskyrimo apibrėžimo, pagal kurį “valstybės neša atsakomybę už pagrindines atakas, kylančias iš valstybės teritorijos ar piliečių”[9]. Šiuo atveju klausimas “kas kaltas” tampa daug svarbesniu ir aktualesniu nei “kas konkrečiai įvykdė ataką”, o priskyrimo problema daug lengviau suvaldoma, kai vietoje iki tol vyravusio “iš apačios į viršų” požiūrio siūloma remtis “iš viršaus į apačią” perspektyva. Ši perspektyva apima ir nevyriausybinius veikėjus, veikiančius valstybės teritorijoje ar su valstybės žinia, kas daugeliu atveju ir yra esminė kliūtis

---

[4] Scott J. Shackelford, “State Responsibility for Cyber Attacks: Competing standards for a growing problem”. Conference on Cyber Conflict, Estonia, 2010.
[5] D. Verton, *Black Ice: The Invisible Threat of Cyberterrorism*. Cambridge: CUP., 2003; J. Ryan, “Countering Militant Islamist Radicalisation on the Internet: A User Driven Strategy to Recover the Web”. Dublin: IIEA, 2007.
[6] D. Hunter, “Cyberspace as Place and the Tragedy of the Digital Anticommons”, California Law Review: 91, 2003, 439-514.; L. Lessig, “The Law of the Horse: What Cyberspace Might Teach*”,* Harvard Law Review:113, 1999, 501-549.
[7] M. N. Schmitt*,* “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework”, Columbia Journal of Transnational Law:7, 1998, 885-937.
[8] Panayotis A. Yannakogeorgos, “Strategies for Resolving the Cyber Attribution Challenge”. Air Force Research Institute Papers, 2013.
[9] Jason Healey, “Beyond Attribution: Seeking National Responsibility for Cyber Attacks”. Atlantic Council, US, 2011.

atsakomybės fiksavimui. J. Healey išskiria valstybės atsakomybės kategorijas, atsižvelgiant į valstybės įsitraukimo intensyvumą[10], taigi valstybės neša atsakomybę netgi tais atvejais, kai atsisako pripažinti išpuolius.

Toks vertinimas yra orientuotas į politikos formavimą, neprisirišant vien prie techninių rodiklių ir pereinant nuo asmeninės atsakomybės prie teisinio legitimizavimo aiškinimo. Juo remiantis nereikalingas tiesioginis („techninis“) kibernetinio išpuolio priskyrimas valstybei, tačiau apeliuojama į efektyvios kontrolės mechanizmą, kuris tampa valstybės atsakomybės sritimi ir potencialiai leidžia įteisinti valstybių atsaką į kibernetines atakas.

David Clark ir Susan Landau savo darbe taip pat akcentuoja, kad siekiant užkirsti kelią atakoms, ypač kompleksinėms atakoms, reikia ieškoti ne tik techninio, bet ir teisinio bei politinio sprendimo.[11] Kibernetinės atakos nebūtinai yra tarpvalstybinio konflikto katalizatorius - daug dažniau, kaip rado ir vieni labiausiai išnagrinėtų atvejų (pvz. Gruzija 2008 m., Estija 2007 m.), tai naudojama kaip „švelnioji“ priemonė, skirta patraukti ir/ar nukreipti valstybės dėmesį. Scott J. Shackelfordo teigimu, nepaisant augančio susidomėjimo atsakomybės priskyrimo galimybe, daugelis studijų yra orientuotos tik į JAV atvejį, kas nėra stebėtina, atsižvelgiant į valstybės mastą ir priklausomybę nuo internetinių tinklų. Kita vertus, tai skatina žiūrėti į mažesnių valstybių atvejus, mažiau nagrinėtus kibernetinius konfliktus ir ieškoti universalesnių kriterijų, kuriais remiantis būtų įmanomas atsakomybės už kibernetinius išpuolius priskyrimas valstybiniu lygiu. Shackelfordas pastebėjo, kad ne tik akademinėje, bet ir teisinėje literatūroje yra akivaizdi spraga apibrėžiant esminius teisinius dokumentus[12], kuriais remiantis būtų galima pradėti derybas atsakomybės tema (kaip pvz. „Talino vadovas“, JT Chartija) taikymo.

Atsakomybės priskyrimas valstybei yra fundamentalus klausimas. Kibernetikos kontekste priskyrimas paprastai laikomas problematišku ir retai išsprendžiamu klausimu dėl techninių parametrų ir neginčytinų įrodymų trūkumo. Tačiau ar iš tiesų atsakomybės priskyrimas yra tiesiogiai susijęs tik su techniniais parametrais? Kaip teigia Thomas Rid ir Ben Buchanan, priskyrimas – tai menas atsakyti į tokius klasikinius klausimus kaip ryšys tarp

[10] Ten pat.
[11] Panayotis A. Yannakogeorgos, “Strategies for Resolving the Cyber Attribution Challenge”. Air Force Research Institute Papers, 2013.
[12] Scott J. Shackelford, “State Responsibility for Cyber Attacks: Competing standards for a growing problem”. Conference on Cyber Conflict, Estonia, 2010.

nusikaltimo ir bausmės: kas tai padarė?[13] Nuo to, kam bus priskirta atsakomybė, priklausys, kuria linkme pasisuks potencialus konfliktas.

Tyrimo tikslas: Remiantis egzistuojančiomis atsakomybės už kibernetinius išpuolius teorinėmis prielaidomis bei praktiniais precedentais bus siekiama nustatyti sąlygas ir aplinkybes, kada valstybė tampa atsakinga už įvykdytas kibernetines atakas bei įvertinti, ar egzistuojančios tarptautinės teisės normos yra pakankamos numatyti valstybių atsakomybę kibernetinių konfliktų atvejais.

J. Healey pasiūlytas valstybės įsitraukimo ir atsakomybės, organizuojant ir vykdant kibernetines atakas, lygmenų skirstymas leis nustatyti ne tik valstybės ryšį su ataka ir jos organizatoriais, bet ir jos pastangas siekiant išvengti atakų pasikartojimo, norą bendradarbiauti su kitais tarptautinių santykių veikėjais. Precedentų ir konkrečių atakų gilesnė analizė leis įvertinti, ar teorija yra pritaikoma praktikoje, pastebėti pasikartojimus, kaip traktuojamos atakos, kokiais teisiniais dokumentais remiamasi, kokie politiniai sprendimai priimami ir koks yra šiuo metu egzistuojantis tarptautinis "bendras sutarimas" dėl atsakomybės apibrėžimo ir priskyrimo valstybei.

Atsakomybės priskyrimui gali būti svarbūs įvairūs faktoriai, pradedant nuo precedento ieškojimo, iki žalos vertinimo remiantis techniniais rodikliais. Daugelis mažesnių atakų taip ir lieka pamirštos, tačiau kai kurios atakos sulaukė tarptautinės bendruomenės dėmesio, buvo nagrinėjamos ir tiriamos, nors iki šiol nėra aišku, ką kaltinti. Pvz. Estija buvo bene pirmųjų, drąsiai viešai prakalbusi ne tik apie išorinę kibernetinę ataką, bet ir tyrimą bei kaltininką. JAV institucijos po pastarųjų prezidentų rinkimų prakalbo apie kibernetinius incidentus rinkimų proceso metu, įvardydama apie turimas žinias, kuri valstybė prie to prisidėjo. Vis dėlto daugeliu atveju nėra oficialių pranešimų, kuri valstybė buvo pripažinta kalta dėl neteisinės veiklos kibernetinėje erdvėje ir kokie to padariniai, t.y. kokios teisės normos bus taikomos valstybei kaltininkei.

Paradoksalu, tačiau nors teisės įgyvendinimas ir kitos teisinės procedūros yra aiškiai apibrėžtos teisinėje literatūroje ir sėkmingai taikomos įvairiems atvejams nagrinėti, kibernetinių atakų priskyrimui praktikų yra gerokai mažiau, nėra aiškiai apibrėžta, kaip jos turi būti traktuojamos ir nagrinėjamos.[14] Žvelgiant į ekspertų diskusijas dėl kibernetinėje erdvėje padarytos žalos priskyrimo konkrečioms valstybėms, taip pat lieka neaišku, kas leidžia, arba priešingai, trukdo identifikuoti valstybės veiklą kibernetinėje erdvėje.

[13] Thomas Rid ir Ben Buchanan, "Attributing Cyber Attacks", Journal of Strategic Studies, 38:1-2, 2015, 4.
[14] Ten pat, 4.

Diskusijų laukui plečiantis, o kibernetinių atakų priskyrimo valstybėms poreikiui augant, vis dar nėra aišku kuo remiantis būtų galima nekvestionuojamai priskirti atsakomybę valstybei.

Darbe keliami šie **uždaviniai**:

1. Apžvelgti teorijas, kurias taikant paranku nagrinėti atsakomybės už įvykdytas kibernetines atakas priskyrimą valstybei;

2. Pristatyti egzistuojančią teisinę baze, taikytiną konfliktas kibernetinėje erdvėje, akcentuojant dokumentus ir sutartis, kuriais remiantis galimas teisinis atsakomybės priskyrimas valstybei;

3. JAV kibernetinės erdvės šnipinėjimas ir įrodymais grįsti kaltinimai Kinijai pasirinktas atvejo studijai. Taikant J. Healey atsakomybės už kibernetines atakas prikyrimo valstybei skalę, siekiama patikrinti, ar šis modelis pritaikomas jau įvykusių kibernetinių atakų ciklui. Taip pat įdomu pastebėti tendencijas, kuo remiantis argumentuojami kaltinimai, kokia "kaltininkės" reakcija, valstybių vieša poziciją incidentų kibernetinėje erdvėje klausimu.

4. Darbo pabaigoje, atlikus atvejo studiją, siekiama pateikti esminius pastebėjimus ir rekomendacijas, ne tik apie modelio privalumus ir trūkumus, bet ir apie valstybių pozicijas dėl atsakomybės valstybei priskyrimo.

Metodika: Atliekama kokybinė atvejo analizė. Jai pasirinktas 2006-2013 m. laikotarpiu trukęs šnipinėjimas kibernetinėje erdvėje, siekiant rinkti JAV žvalgybos, diplomatinio korpuso, ekonomikos ir gynybos sektorių informaciją. Šių kibernetinių atakų kaltininke, 2013 m. Pentagono metinėje ataskaitoje įvardyta Kinija, neteisėtais veiksmais siekianti išgauti naudingą informaciją, kuria galėtų pasinaudoti kuriant savo gynybos programą. Glaustai chronologiškai pristatomos kibernetinės atakos, kurios, remiantis oficialiais pranešimais, yra priskiriamos Kinijos vyriausybei, apžvelgiama kaip Kinija apibrėžia kibernetinės erdvės suverenitetą, kokią teisinę bazę taiko kibernetiniams konfliktams. Siekiant taikyti J. Healey pasiūlytą valstybės atsakomybės dėl kibernetinių atakų spektrą, atliekama pirminių (viešai prieinamas Mandiant, privačios kibernetinio saugumo kompanijos, ir Pentagono metinis pranešimas) ir antrinių (t.y. ekspertų įžvalgos, naujienų pranešimai ir t.t.) šaltinių analizė. Svarbu paminėti, jog JAV kaltinimus Kinijai grindžia oficialiais pranešimais, remdamasi Mandiant atliktu tyrimu, tuo tarpu pirminių šaltinių iš Kinijos perspektyvos rasti sudėtinga. Autoritarinis valdymas, griežta spaudos kontrolė ir interneto filtravimas mažina pateiktos informacijos prieinamumą ir patikimumą.

1. Teorinės prielaidos atakų kibernetinėje erdvėje analizei

Laikotarpiu, kai valstybės susiduria su įvairaus tipo grėsmėmis iš išorės, atsakomybės už atakas kibernetinėje erdvėje priskyrimas išlieka esminiu saugumo užtikrinimo klausimu. Laikantis konstruktyvistinės perspektyvos „atsakomybė“ turėtų būti suvokiama kaip socialinėmis praktikomis ir diskursu konstruojama sąvoka, o ne kaip objektyvi duotybė.[15] Atsakomybės priskyrimo problemą galima spręsti tiek valstybės, tiek tarptautiniu lygiu, pavyzdžiui, kuriant tarptautinius teisinius įsipareigojimus. Vis dėlto tik konkrečiai nustatyti kriterijai gali padėti išvengti pernelyg plačių interpretacijų dėl atsakomybės priskyrimo.

Diskusijose apie priskyrimą kibernetinėje erdvėje dominuoja trys pagrindinės srovės, kodėl nepavyksta sėkmingai priskirti atsakomybės valstybėms. Pirmiausia, tai prielaida, kad priskyrimo problema yra nesuvaldoma dėl interneto specifikos, sudėtingų techninių parametrų ir konkretaus išpuolio geografijos nustatymo, todėl vienintele išeitimi laikomas interneto perprojektavimas, tiek iš techninės, tiek teisinės perspektyvos. Tačiau internetas nuo pat tinklo sukūrimo nebuvo skirtas vartotojų identifikavimui, todėl prieštarautų pačiai tinko naudotojo koncepcijai. Kadangi internetas visų pirma užtikrina anonimiškumą, o ne saugumą, siekis sekti nepatikimus vartotojus nebūtų sėkmingas.[16]

Antroji prielaida - tai dvilypis požiūris į priskyrimą, kuomet bet kurio internetinio incidento atvejo tyrimas turi baigti problemos išsprendimu (o dar dažniau neišsprendimu). Arba kaltininkas yra aiškiai įvardijamas (grindžiant neginčytinais įrodymais), arba bylos numarinimu trūkstant įrodymų. Šiuo atveju galima galvoti tiek apie techninį (ne)pasirengimą atlikti gilesnį nei vien IP adresų nustatymą, tiek apie politinės valios trūkumą.

Trečioji prielaida, jog svarbiausias priskyrimo elementas yra įkalčių radimas, o ne jų analizė, glaudžiai siejasi su antrąja.

Šie požiūriai yra intuityvūs ir patys savaime nėra klaidingi, tačiau labai riboti, nors priskyrimo problema per pastaruosius dešimtmečius sparčiai kito, kibernetiniams išpuoliams dažnėjant, jiems tampant vis labiau politizuotiems, plėtėsi ir tyrimų laukas.[17] Dėl įsitikinimo, kad neįmanoma objektyviai ir nekvestionuojamai įvertinti, kokie veikėjai, organizacija ar

[15] Peter L. Berger ir Thomas Luckmann, *The Social Costruction of Reality*. Penguine Books, 1966. <http://perflensburg.se/Berger%20social-construction-of-reality.pdf>

[16] Interneto specifika- Jason Healey, “Beyond Attribution: Seeking National Responsibility for Cyber Attacks”. Atlantic Council, US, 2011. ir Scott J. Shackelford ir Richard B.Andres, “State Responsibility for Cyber Attacks: Competing standards for a growing problem”. Conference on Cyber Conflict, Estonia, 2010.

[17] Prielaidos- Thomas Rid ir Ben Buchanan, “Attributing Cyber Attacks”, Journal of Strategic Studies, 38:1-2, 2015, 4.

valstybė įvykdė išpuolį kol nebuvo atlikta techninė ekspertizė, atsakomybės priskyrimo problema taip ir lieka nesprendžiama, iš naujo grįžtama prie būtinybės rasti techninius kriterijus, pakankamus ir nekvestionuojamus, todėl leidžiančius teikti aiškų sprendimą.

Vis dėlto tiek tarptautinei saugumo bendruomenei, tiek nacionalinės saugumo politikos formuotojams svarbesnis yra ne klausimas, koks konkrečiai individas ar grupė įvykdė kibernetinį išpuolį, o kas dėl to turėtų būti apkaltintas, t.y. kam už tai tenka atsakomybė.[18] Kaip nurodo J. Healey, tarptautinė bendruomenė turi atitinkamai perskirstyti resursus nuo techninės perspektyvos siekiant identifikuoti atakos kaltininkus, į atsakomybės priskyrimo problemą. Sprendžiant šią problemą galima pasitekti plataus spektro įrankius: nuo diplomatijos, žvalgybos, iki karinių pajėgų, ekonominių sankcijų ir t.t.[19]

Tomašas Bruneris, remdamasis įvairių autorių darbais, siūlo į atsakomybę žiūrėti per vertikalią ir horizontalią perspektyvas. Galima tiek vidaus lygmens analizė, tiek analizė per valstybių tarptautinį bendradarbiavimą ir kooperavimąsi. Vertikalus modelis arba M. Koskenniemio vadinama "komunitarinė doktrina" numato pareigą tarptautinei bendruomenei priskirti atsakomybę nacionalinei valstybei, bet taip pat ir valstybės piliečiams bei visiems žmonėms pagal savo jurisdikciją. Šis modelis sujungia valstybės atsakomybę su vadinamąja "kategoriškumo taisykle", kuri paverčia tam tikras normas privalomomis *erga omnes* (taikytinos visiems bendruomenės nariams). Modelis taip pat akcentuoja, kad atsakomybė turi išreikšti tautos, o ne valstybės interesus (tarnauti tautos valiai siekiant užtikrinti jos saugumą).[20]

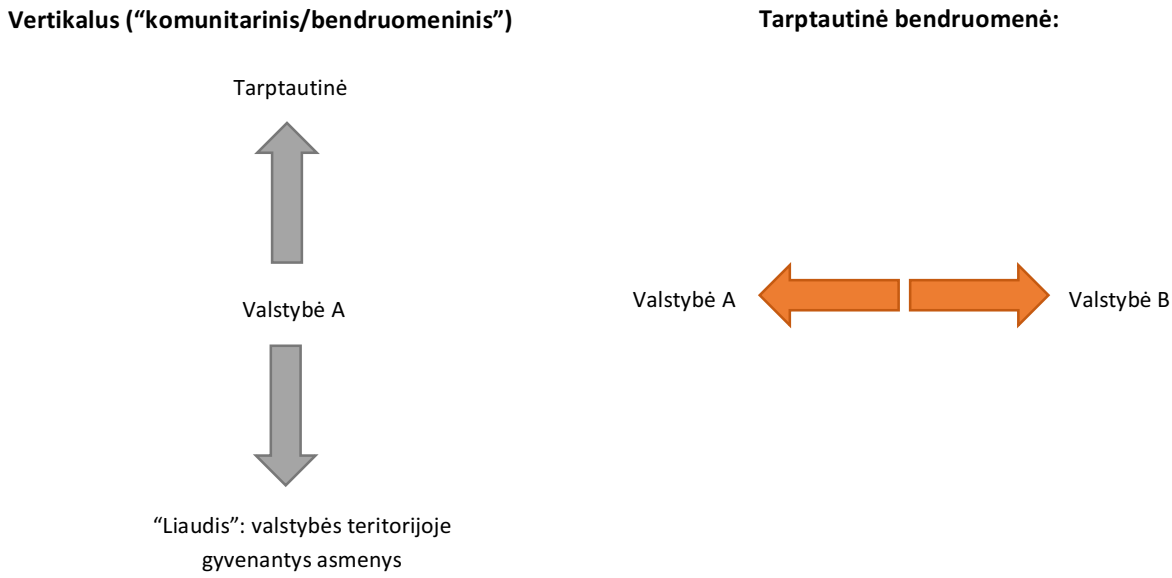
Priešingai, remiantis horizontaliuoju modeliu, valstybės atsakomybė suprantama tik kalbant apie dvišalius santykius tarp valstybių. Šis modelis yra vidaus lygmens analizės analogas (autoriai siūlo supaprastintai įsivaizduoti du piliečius, siejamus tam tikrų teisinių santykių, kas reiškia, kad jie abu turi teises ir pareigas vienas kito atžvilgiu), taigi valstybė yra atskaitinga tik prieš kitą dvišalių santykių dalyvį, t.y. kitą valstybę, saistomą tų pačių atsakomybių. Pasak šio modelio, tarpusavio atsakomybė yra natūralus valstybių egzistavimo rezultatas. Vertikalaus modelio taikymas labai lankstus, tuo pačiu išlieka galimybė reaguoti į dvišalių santykių pažeidimus tarptautiniu lygiu. Šis metodas buvo palankiai vertinamas klasikinės tarptautinės teisės teoretikų. H. Lauterpachto teigimu, kai valstybė yra pakankamai galinga, kad užtikrintų savo egzistavimą, kitos valstybės turi ją pripažinti. Taigi tokiu būdu

[18]Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks". Atlantic Council, US, 2011, 1.
[19] Ten pat, 1.
[20] Philip Allot, "State Responsibility and the Unmaking of International Law". Harvard International Law Journal. Volume 29, No. 1., 1988, 26. Iš Tomaš Bruner, "States in Cyber-Space: Perspectives of Responsibility Beyond Attribution", 4.

valstybė gali sudaryti sutartis su kitomis valstybėmis. Tuo pat metu ji yra atsakinga prieš jas dėl netinkamo, neteisinio ir žalingo elgesio.[21]

Šie du modeliai gali būti suvokiami kaip tarpusavyje konkuruojantys arba M. Weberio idealieji tipai. Jų bruožų galima pastebėti skirtinguose teisiniuose diskursuose, kartais jie gali susimaišyti, vienas ryškėti, kitas nykti. Netgi neesminiuose teisiniuose dokumentuose apie valstybės atsakomybę, kaip pvz. „Valstybių atsakomybės už tarptautinius neteisėtus aktus“ straipsnių projekte[22] atsakomybė gali būti analizuojama tiek per horizontalią, tiek per vertikalią perspektyvą.[23] Apskritai linkstama manyti, kad nors tradicinė tarptautinė teisė laikosi horizontalaus modelio idėjos, modernioji tarptautinė teisė linkusi taikyti vertikalųjį (komunitarinį/bendruomeninį) modelį, todėl darbe pasirinkta remtis būtent pastaruoju, kaip ryškiau atsispindinčiu teisiniuose dokumentuose, nagrinėjančiuose atsakomybės kibernetinėje erdvės priskyrimui problematiką.

Valstybės atsakomybės schema:



Lentelė nr.1. Pagal Tomaš Bruner, “States in Cyber-Space: Perspectives of Responsibility Beyond Attribution”.

Siūlymai į problemą žiūrėti iš viršaus į apačią, o ne iš apačios į viršų (kai valstybės atsakingos už atakas iš jos teritorijos arba vykdomos jos piliečių) nėra nauji ir pastaruoju

[21] Hersch Lauterpacht,, “Recognition of States in International Law”. The Yale Law Journal. Vol. 53, No. 3, 1944. Iš Tomaš Bruner, “States in Cyber-Space: Perspectives of Responsibility Beyond Attribution”, 5.
[22] Draft Article on Responsibility of States for Internationally Wrongful Acts, 2001. <http://untreaty.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf>
[23] Martti Koskenniemi, “Doctrines of State Responsibility”, 2010. Iš James Crawford, Pellet, Alain Olleson, Simom, “The Law of International Responsibility”. New York, Oxford University Press: 2010. Iš Tomaš Bruner, “States in Cyber-Space: Perspectives of Responsibility Beyond Attribution”, 4-5.

metu įgauna pagreitį. Jason Healey siūloma alternatyva - atsižvelgiant į kibernetinių grėsmių specifiką plačiau pažiūrėti į priskyrimo klausimą, įtraukiant ir nevyriausybinius veikėjus, kai valstybės atsakingos už pagrindines atakas, kylančias iš jos teritorijos ar vykdomos jos piliečių. Jis pateikia valstybių atsakomybės lygmenų spektrą, kaip įrankį priskirti atsakomybės už išpuolį „laipsnį“, kur skirtingas laipsnis priklauso nuo to, ar valstybė ignoruoja, bendrininkauja/tarpininkauja ar vykdo puolimą. Autorius pasiūlo išskirti valstybės atsakomybę į kategorijas, atsižvelgiant į valstybės įsitraukimo intensyvumą (valstybės indelį kylant kibernetinei atakai):

1. **Valstybė draudžia kibernetines atakas** – valstybės vyriausybė padeda sustabdyti trečiosios šalies atakas.
2. **Valstybės draudžia, bet ne pakankamai** – valstybės vyriausybė bendradarbiauja siekiant sustabdyti atakas, bet nėra pajėgi sustabdyti trečiosios šalies atakų.
3. **Valstybė ignoruoja** – valstybės vyriausybė turi žinių apie trečiosios šalies atakas, bet nenori imtis jokių oficialių veiksmų.
4. **Valstybė skatina** - politikos priemonė, kai trečioji šalis planuoja ir vykdo atakas, o valstybės vyriausybė tokius veiksmus skatina.
5. **Valstybė formuoja** - trečioji šalis planuoja ir vykdo atakas, o valstybės vyriausybė jas iš dalies remia.
6. **Valstybė koordinuoja** - valstybės vyriausybė koordinuoja trečiosios šalies veiksmus, pvz. teikdama pasiūlymus jų įgyvendinimui (operaciniame lygmenyje).
7. **Valstybė užsako** - valstybės vyriausybė nukreipia trečiosios šalies veiksmus, taigi jie vykdomi jos vardu.
8. **Valstybės vykdoma užslėptai** - valstybės vyriausybės nekontroliuojami kibernetiniai veikėjai vykdo atakas.
9. **Valstybės vykdoma (tiesiogiai)** - valstybės vyriausybė planuoja ataką, naudodama kibernetines pajėgas, esančios jos žinioje.
10. **Valstybė įsitraukusi** - valstybės vyriausybė atakuoja naudodamasi integruotais trečiųjų šalių ir valstybiniais pajėgumais.[24]

Remiantis nurodytomis atsakomybėmis formomis galima išskirti „pasyvią“ ir „aktyvią“ atsakomybę. Pasyvios atsakomybės priskyrimas apima valstybes, turinčias nesaugias sistemas, kurios veda link atakos, tuo tarpu aktyvi atsakomybė apeliuoja į nacionalines vyriausybes, kurios iš tikrųjų planuoja ir vykdo atakas. Valstybės, patenkančios į pirmas dvi

[24]Jason Healey, “Beyond Attribution: Seeking National Responsibility for Cyber Attacks”. Atlantic Council, US, 2011, 2-3.

kategorijas turi labai pasyvią atsakomybę, kadangi bando kooperuotis ir komunikuoti su ataką patyrusia valstybe, o aukštesnio laipsnio kategorijos rodo gilesnį valstybės įsitraukimą.[25]

Valstybės draudžiamomis atakomis laikytinos tokios atakos, kurios prieštarauja valstybės teisės normoms, tačiau nepaisant to, atakos įvyksta. Tokiu atveju, kai atakos vyksta nepaisant valstybės draudimų, valstybė nepažeidžia atsakomybės užkirsti kelią naudotis savo teritorija atakai prieš kitą valstybę ir netgi gali sulaukti tarptautinės bendruomenės paramos. Atsisakymas suteikti paramą tarptautinėms institucijoms, kitoms valstybėms ar tyrėjams, kad būtų užkirstas kelias naujiems ar pasikartojantiems išpuoliams, kitą vertus, būtų požymis, kad valstybė nėra linkusi bendradarbiauti.[26] Taigi, remiantis šiuo spektru, valstybės tampa atsakingomis atsisakydamos pripažinti išpuolius, atsisakydamos siūlomos pagalbos juos tiriant ar stabdant atakas iš jos teritorijos. Pasak spektro autoriaus, juo galima remtis tiek siekiant apibūdinti pavienes atakas, tiek susijusių atakų virtinę. Spektras skirtas kibernetinės erdvės gynėjams (kai ataka yra užsakyta, valstybei buvo siūloma bendradarbiauti, bet jai atsisakius, saugumo užtikrinimo būtinybė pereina į nukentėjusiosios rankas) ir politinei bendruomenei (valstybės politika yra paremta atskaitomybe, kiekviena prieš valstybę nukreipta ataka turi būti priskirta kaltininkei).[27]

Spektras ir kategorijos jame labai lanksčios, todėl bet kuri kibernetinių išpuolių kampanija tiks bent vienam iš įvardytų kriterijų. Jis gali būti naudojamas kaip įrankis, padedantis analitikams su nepilna informacija priskirti atsakomybę dėl atakos daug tiksliau. Atsižvelgiant į kibernetinės erdvės specifiką, suprantama, kad valstybės negali pilnai kontroliuoti kibernetinės erdvės, kaip kad oro erdvės ar vandenų teritorijos. Visgi dabartinė situacija rodo, kad tarptautinė bendruomenė traktuoja visas kibernetines atakas, lyg jos būtų vykdomos iš žlugusios valstybės (*failed state*), nepajėgios atsakyti už iš jos suverenios teritorijos kylančius veiksmus. Situacija turėtų būti priešinga, kaip teigia David Grahamas, valstybės pačios turėtų būti suinteresuotos, kad jų teritorija nebūtų naudojama kaip "saugus rojus" ir kooperuotis, siekiant tirti ir įvardyti tarptautinių kibernetinių atakų kaltininkus.[28]

Toks požiūris leidžia stebėti, kiek stipriai valstybė prisideda prie kibernetinių atakų mažinimo ir kontrolės priskyrimo mechanizmo tobulinimo. Panayotis A. Yannakogeorgos,

[25]Ten pat, 3.
[26]Panayotis A. Yannakogeorgos, "Strategies for Resolving the Cyber Attribution Challenge". Air Force Research Institute Papers, 2013, 55-56.
[27] Ten pat, 55-56.
[28]Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks". Atlantic Council, US, 2011, 5.

savo darbe kalbėdamas apie iššūkius, su kuriais susiduriama siekiant priskirti atsakomybę valstybei, J. Healey spektrą pateikė kaip lentelę, įtraukdamas pagalbos, diplomatijos ir gynybos elementus. Schematiškas spektro vaizdavimas patogus atvejo studijai, todėl darbe bus naudojama lentelė su pagalbos (ar valstybė turi žinių apie galimą pasiruošimą atakai iš jos teritorijos, kibernetinės infrastruktūros egzistavimą ir vystymą) ir diplomatijos (ar egzistuoja dvišaliai ar daugiašaliai susitarimai, tiesinė bazė, draudžianti kibernetinius nusikaltimus) elementais, tačiau atsisakant gynybos elemento, kadangi pirminis darbo tikslas yra rasti sąlygas atsakomybei priskirti. Svarbu paminėti, kad Panayotis A. Yannakogeorgos pateikta lentelė su trimis elementais (pagalba; diplomatija; gynyba) buvo taikoma JAV atvejo analizei, siekiant patikrinant, kiek pritaikoma J. Healey pateikta schema realiai įvykusioms atakoms analizuoti ir ar JAV yra pasirengusi į jas atsakyti. Autorius elementus tikrina naudodamasis 2011 m. Baltųjų rūmų tarptautine Kibernetinės erdvės strategija, kurios tikslas buvo per JAV iniciatyvą pasiūlyti tarptautiniu lygiu taikytinas normas, reaguojant į kibernetines atakas. "Pagalba" apibrėžiama kaip valstybės gebėjimas užtikrinti kibernetinių incidentų tyrimą, jeigu valstybei to pasiekti pačiai nepavyksta dėl techninių pajėgumų ar patirties trūkumo, Strategijoje įtvirtintas siekis suteikti reikalingą pagalbą.[29] Tuo tarpu "diplomatijos" elemente akcentuojama regioninio ir tarptautinio bendradarbiavimo svarba, paremta tarpusavio pasitikėjimu, taip ne tik siekiant vystyti bendrus pajėgumus saugumui kibernetinėje erdvėje užtikrinti, bet ir dalintis gerąja praktika, mokytis vieni iš kitų.[30]

Panašios analizės, peržiūrint skirtingų valstybių kibernetines atakas ir daugiau egzistuojančių teisinių dokumentų, orientuotų į kibernetinės erdvės gynybą, nebuvo atlikta, todėl prasminga bandyti pritaikyti autoriaus siūlomą schemą su J. Healey įsitraukimo diapazonu platesniam kontekstui.

[29] Panayotis A. Yannakogeorgos, "Strategies for Resolving the Cyber Attribution Challenge". Air Force Research Institute Papers, 2013, 57-58.
[30] Ten pat, 58-59.

Valstybės veiklos diapazonas		Pagalba	Diplomatija	Gynyba
	Valstybė draudžia kibernetines atakas			
	Valstybė draudžia, bet ne pakankamai			
	Valstybė ignoruoja			
	Valstybė skatina			
	Valstybė formuoja			
	Valstybė koordinuoja			
	Valstybė užsako			
	Valstybės vykdoma užslėptai			
	Valstybės vykdoma (tiesiogiai)			
	Valstybė įsitraukusi			

Lentelė nr. 2. Sudaryta remiantis Jason Healey "Beyond Attribution: A Vocabulary for National Responsibility for Cyber Attacks" ir Panayotis A. Yannakogeorgos "Strategies for Resolving the Cyber Attribution Challenge" pateiktomis schemomis.

Vyrauja įsitikinimas, kad atsakomybės priskyrimas yra siekis "išspręsti neišsprendžiamą" arba tai, ką valstybėms pavyksta iš jo "išspausti". Patvirtindami šį teiginį Thomas Ridas ir Ben Buchananas pateikė Q modelį[31], kuris papildo J. Healey atsakomybės priskyrimo valstybei spektrą ir yra tolimesnis atsakomybės priskyrimo etapas. Kadangi sutarta, kad atsakomybės klausimą reikia perkelti valstybei taip įtraukiant ir nevyriausybinius veikėjus, šis modelis padeda rasti ryšį tarp nusikaltimo ir nusikaltėlio, o neapibrėžtumas ir neužtikrintumas mažinamas trijų lygmenų priemonėmis: taktiniu, operaciniu ir strateginiu.

Jeigu laikysime, kad priskyrimas neturėtų remtis vien techniniais rodikliais, tuomet kyla klausimų, kuo remiantis galima užtikrinti nekvestionuojamą priskyrimą. Kaip jau buvo išskyręs ir Jason Healey, galima teigti, kad priskyrimas priklauso nuo valstybės įsitraukimo į ataką lygmens (J. Healey atveju išskirtas kaip spektras). Tačiau nustačius valstybės vaidmenį prisidedant prie kibernetinės atakos tampa svarbus politinio elito vaidmuo. Nuo jų

[31] Thomas Rid ir Ben Buchanan, "Attributing Cyber Attacks", Journal of Strategic Studies, 2015, 38.

sugebėjimo priimti realų politinį sprendimą ir iškelti atsakomybės priskyrimo klausimą tarptautiniu lygiu priklauso galimybės reikalauti teisinės ir politinės atsakomybės.

Detaliau pažvelgus į autorių siūlomą modelį tampa aišku, kad kiekvienas atsakomybės priskyrimo proceso lygmuo yra glaudžiai tarpusavyje susijęs, remiasi skirtingai iššūkiais ir reikalauja skirtingų duomenų bei patirčių, siekiant rasti atsakymus į to lygmens klausimus bei pereiti į kitą. Nors priskyrimo procesas paprastai turi pradžią ir pabaigą, ciklas ne būtinai turi sekti nustatyta tvarka ar chronologine seka. Sluoksniai reprezentuoja atskiras užduotis, ir nors jie persidengia, kiekvienas sluoksnis turi būti nagrinėjamas atskirai. Paprastai taip vadinamas "kompromiso indikatorius" paskatina priskyrimo procesą plėtotis - atsiranda naujų faktų, kyla nauji klausimai ir t.t. Kartais pasitaiko situacijų, kai priskyrimo procesas prasideda operaciniame ar strateginiame lygiuose. Tokiu atveju pradinės žinios apie incidentą ateina ne iš techninių rodiklių, pateikiamų IT administratorių, o neoficialių žvalgybinių pranešimų, platesnio geopolitinio konteksto, taigi galimai netgi intuicijos, esant galimybei identifikuoti kenkėjiškus veiksmus, prieš juos patvirtinant techniniais rodmenimis arba netgi sustabdyti prieš jiems prasidedant. Taigi priskyrimas gali judėti bet kuria kryptimi: iš strateginio ir operacinio lygmens kylantis poreikis techninėms detalėms ir vice versa.[32]

Priskyrimo procesas yra glaudžiai susijęs su potencialia žala, kas akcentuojama ir vėliau aptariamuose teisiniuose dokumentuose, nagrinėjančiuose kibernetinių ataką problematiką. Jeigu veiksmai nesukėlė jokios akivaizdžios žalos, kompanija ar valstybė gali nuspręsti nesiimti tyrimo, o pvz. investuoti į IT sistemos tobulinimą ar gynybą, siekiant išvengti galimų pasikartojančių atakų. Šiuo atveju į žalą reiktų žiūrėti plačiau nei fizinė žala infrastruktūrai. Žala galima laikyti ir grasinimus, šantažą, informacijos, neskirtos viešinimui paskelbimą, propagandą ir pan. Žala gali būti tiesioginė (pvz. sulėtinti serverių darbą ir sumažinti prieinamumą prie failų), netiesioginė, šiuo atveju tai - reputacijos ar patikimumo praradimas, taip pat žala gali būti netiesioginė ir patiriama po tam tikro laiko, t.y. uždelsta (pvz. intelektinė nuosavybė ir iškreipta rinkos konkurencija, kai nukentėjusysis su savo produktu tampa nekonkurencingas rinkoje).[33] Tokiu atveju priskyrimo procesas gali sustoti net neprasidėjęs, tačiau tam tikras skaičius tokių incidentų yra neišvengiamas. Modelio autorių teigimu, taktiniame lygmenyje kiekvieno incidento suvokimas prasideda techniniais aspektais, t.y. *kaip* lygmeniu. Operacinio lygmens tikslas yra perkelti koncentraciją iš klausimo *kaip (tai įvyko)* į kaip *kas (tai padarė)*, t.y suprati atakos pobūdį bei kenkėjo profilį. Tuo tarpu strateginis lygmuo padeda rasti *kas yra atsakingas* (*ką dėl to kaltinti*) už ataką, bei

[32] Ten pat, 7-8.
[33] Ten pat, 24-25.

įvertinti jos tikslą, reikšmę, paskirtį, siekiant rasti tinkamą atsaką, t.y. atsakyti į klausimus *kas atsakingas* ir *kodėl*.[34]

Autoriai pateikia schematišką ir labiau išplėtota J. Healey idėją, jog kibernetikoje atsakomybės priskyrimas juda link tikslo rasti *kas atsakingas*. Q modelyje taip pat atsiranda ir naujas, atskiras dėmuo - komunikacija, kaip atskiras tikslas. Komunikacija yra plataus masto tyrimo ir ekspertizės rezultatas, viešas apdorotos turimos informacijos pateikimas gali turėti neginčytiną rezultatą - galimai nutraukti būsimą ataką, skatinti kenkėjus keisti taktiką, viešai reaguoti į pateiktus įrodymus ir t.t.[35] Todėl modelio autoriai ne kartą mini detalių svarbą, detalės bet kuriame etape gal pagerinti atsakomybės prikyrimą. Kai atvejo detalės yra paviešinamos, priskyrimo kokybė (tikslumas) išauga. Tokiu pavyzdžiu galima laikyti inovatyvią kolektyvinę *Stunex* kodo analizę - skirtingos kompanijos ir tyrimų institutai analizavo kenkėjišką programą ir pateikė plačią, detalią ataskaitą, fokusuodamiesi ties skirtingais operacijos aspektas, kas leido susidaryti vaizdą iš skirtingų perspektyvų.[36] Paradoksalu, tačiau atvirumas priskyrimo procese užtikrina geresnį kolektyvinį saugumą. Rastų detalių dalinimasis naudingas ne tik konkretaus atvejo studijai, bet bendrai kolektyviai gynybai ir jos tobulinimui. Tiek iš techninės perspektyvos, pvz. tobulinant infrastruktūrą, tiek ir kaip tarptautinė bendruomenė priima ir reaguoja į pateikimą informaciją. Nepaisant to, jog modelis pirmiausia akcentuoja perėjimą nuo koncentracijos ties techninėmis detalėmis prie atsakomybės priskyrimo, ieškant kas dėl to kaltas, techninės detalės išlieka itin svarbios, informacija, kuri cirkuliuoja techniniame, operaciniame ir strateginiame lygmenyse turi būti susintetinta, tik tuomet ji bus suprantama ir naudinga.

Autorių studija - tai konceptualus praktinis žemėlapis, padedantis suprasti priskyrimo proceso eigą, nuo tyrimo elementų, iki galutinio rezultato, nuo žvalgybos darbo rezultatų iki nacionalinio saugumo užtikrinimo institucijų, politinių lyderių sprendimų. Taktine prasme, šis modelis padeda analitikams užduoti visus reikalingus klausimus, paskatina kritinį mąstymą ir "pastumia" tyrimą priklausomai nuo konteksto. Operaciniame lygmenyje, remiantis modeliu, tiek techninės, tiek ne techninės hipotezės gali tarpusavyje konkuruoti ir viena kitą papildyti, taigi klausimai gali tapti daug sudėtingesni su smulkmeniškomis detalėmis, apimantys skirtingas kategorijas, pereinantys į pasiūlymus. Strateginiame lygmenyje, remiantis modeliu, galima išgryninti priskyrimo procesą, ypač aktualu prieš

[34] Ten pat, 10-11.
[35] Ten pat, 10-11.
[36] Ten pat, 28.

pateikiant įžvalgas poliniam elitui, priimančiam sprendimus.[37] Taigi modelis gali būti taikomas paraleliai su valstybės įsitraukimo schema arba jau žinant valstybės indėlį į ataką ir siekiant rasti tolimesnius galimus ėjimus, kurie problemą iškelti į tarpvalstybinį lygmenį.

Anot autorių, priešingai nei manyta, priskyrimo kokybė tiesiogiai priklauso nuo teisingai užduotų klausimų, ne nuo techninių rodiklių. Šis procesas yra dinamiškas, kiekviena valstybė ir kiekvienas atvejis yra skirtingas, todėl sunku kalbėti apie galima kontrolinį sąrašą. Autorių studija per Q modelį pateikia schemą, kaip kibernetinės atakos gali būti priskirtos valstybėms, nepaisant anksčiau minėtų trijų vyraujančių nuostatų.

Priskyrimo procesas yra menas, sudėtingas, kompleksiškas, daugiasluoksnis, o ne mechaniškas, techniškas ir rutiniškas procesas. Aukščiausio lygmens, taigi neabejotino atsakomybės priskyrimo galima pasiekti tik žiūrint "iš paukščio skrydžio", sėkmė priklauso nuo dėmesio detalėms, techninių pajėgumų, ekspertų pasirengimo, tarptautinės aplinkos suvokimo, netgi vidinio "kažkas ne taip" jausmo, skatinančio tęsti tyrimą. Politinė valia vaidina svarbų vaidmenį šiame procese, bet koks atsakas į priešišką veiksmą reikalauja nustatyti pažeidėją. Valstybės nusprendžia kada atsakomybės priskyrimas yra pakankamas, kad būtų galima imtis veiksmų, tačiau bendras sutarimas dėl pradinių detalių, leidžiančių pradėti tyrimą yra būtinas.[38]

2. Teisiniai kibernetinės atsakomybės aspektai

Kibernetinio saugumo problematika šiuo metu yra visų didžiųjų valstybių ir daugumos mažesnių, patyrusių ar jautusių tokių atakų grėsmę valstybių (Nyderlandai, Estija, Lietuva, Izraelis) nacionalinio saugumo strategijose. Nacionaliniu ir tarptautiniu lygiu siekiama apibrėžti kibernetines grėsmes, kibernetinių grėsmių tipus, riziką, ieškoti pasikartojimų ir prevencijos ar kovos su kibernetinėmis atakomis būdų. Kibernetinių atakų grėsmė jau keletą metų yra aptariama tokiose viršnacionalinėse organizacijose kaip Europos saugumo ir bendradarbiavimo organizacija (ESBO), pvz. 2010 m. ESBO politinių vadovų susitikime buvo kalbama apie naujai iškylančias tarptautines grėsmes ir būtinybę kurti

[37] Ten pat, 7.
[38] Ten pat, 7.

saugumo bendruomenę, siekiant užtikrinti kolektyvinį saugumą[39], tačiau konkrečių kibernetinio saugumo užtikrinimo rekomendacijų iki šiol nėra pateikta.

Remiantis J. Healey modeliu ir nustačius valstybės įsitraukimo lygį bei laikantis teiginio, jog daug svarbesniais nei kompiuterių kodai tampa fizinis, loginis, informacinis ir žmogiškasis faktorius kibernetikoje, svarbu apžvelgti, kaip remiantis egzistuojančia tarptautine teise galima reaguoti į tarptautinės teisės principų ir normų pažeidimus. Pagal viešąja tarptautinę teisę, bet koks valstybes įvykdytas tarptautinės teisės pažeidimas užtraukia šios valstybės tarptautinę atsakomybę. Šis iš paprotinės teisės kilęs principas atsispindi 2001 m. JT Tarptautinės teisės komisijos patvirtinto Valstybių atsakomybės už tarptautinius neteisėtus aktus straipsnių projekte.[40] Tarptautinės teisės pažeidimu, remiantis dokumento 2 straipsniu laikoma: "Valstybė įvykdo tarptautinės teisės pažeidimą, kai jos veika, pasireiškianti veikimu ar neveikimu: (a) priskiriama šiai valstybei pagal tarptautinę teisę ir (b)yra šios valstybės tarptautinio įsipareigojimo pažeidimas."[41] Taigi valstybės atsakomybė apima du elementus: objektyvų ir subjektyvų. Objektyvus elementas suponuoja į konkrečios normos pažeidimą, subjektyvus elementas reiškia, kad tokio elgesio kaltininkas gali būti identifikuotas, kitaip tariant, įvykdytas veiksmas gali būti jam priskirtas. Valstybė yra atsakinga už tam tikrą veiksmą ar neveikimą, jeigu šis veiksmas pažeidžia tam tikra konkrečią tarptautinės teisės normą ir yra tikėtina, kad buvo atliktas valstybės. Kitas svarbus atsakomybės aspektas, įvardytas dokumento 8 straipsnyje "Elgesys, kuriam vadovauja ar kurį kontroliuoja valstybė" - "Asmens ar asmenų grupės elgesys laikomas valstybės veika pagal tarptautinę teisę su sąlyga, kad šis asmuo ar ši asmenų grupė faktiškai veikia vykdydami valstybės instrukcijas arba jos vadovaujami ar kontroliuojami tokio elgesio metu."[42] Remiantis šiuo straipsniu ir Healey spektro punktais, valstybė tampa pilnai atsakinga už įvykdytus veiksmus, net jeigu pati tai neigia. Tačiau šiuo atveju "kontrolės" sąvoka nėra aiškiai apibrėžta, todėl sprendimas paliekamas teismų interpretacijai ir veda link diskusijų apie efektyvios ir bendrosios kontrolės testų taikymą, kurie bus aptarti vėliau.

Pagal 14 straipsnio 3 punktą, "Valstybės tarptautinio įsipareigojimo, kuris reikalauja, kad valstybė užkirstų kelią tam tikram įvykiui, pažeidimas įvyksta tada, kai

[39] Organization for Security and Co-operation in Europe, "The Astana Commemorative Declaration: Towards a Security Community", sum.doc./1/10//Corr.1, 2010 m. gruodžio 3 d. <http://www.osce.org/cio/74985?download=true>
[40] Vilenas Vadapalas, "Tarptautinė teisė. Pagrindiniai dokumentai ir jurisprudencija". Vilnius, Eugrimas, 2003, 258.
[41] Ten pat, 258
[42] Ten pat, 260.

šis įvykis įvyksta ir tęsiasi visą laikotarpį, kurį šis įvykis vyksta ir neatitinka šio įsipareigojimo."[43], taigi valstybės nesikišimas turint žinių apie kenkėjišką veiklą taip pat gali būti klasifikuojamas kaip tarptautinės normos pažeidimas. Lygiai taip pat valstybės neveikimas, pastangų nutraukti nusikalstamą veiklą ir užkirsti kelią nebuvimas yra laikytinas pažeidimu. Remiantis 30 straipsniu "Pažeidimo nutraukimas ir nepakartojimo garantijos" - "Valstybė, atsakinga už tarptautinės teisės pažeidimą, privalo: a) nutraukti šią veiką, jei ji tęsiasi; jei aplinkybės to reikalauja, tinkamai užtikrinti ir garantuoti, kad pažeidimas nebus pakartotas."[44] Nei vienas iš anksčiau minėtų straipsnių negali būti paneigtas, argumentuojant vidaus teise, nes "Atsakinga valstybė negali remtis savo vidaus teisės nuostatomis tam, kad pateisintų savo įsipareigojimų pagal šią dalį nesilaikymą".[45]

Istoriškai, kalbant apie valstybės atsakomybę buvo laikomasi idėjos, jog valstybė yra atsakinga tik už savo ar veiksmus, atliktus paramilitarinių ir kitų nevalstybinių veikėjų remiantis tiesiogine kontrole. Dažnėjant neidentifikuotų nevyriausybinių veikėjų sukeliamų incidentų, kas lemia nesėkmingą neteisėtų veiksmų priskyrimą valstybei, augo poreikis pokyčiams tarptautinėje teisėje. Nusigręžiama nuo tradicinių reikalavimų, keliamų siekiant priskirti atsakomybę valstybei, pereinama prie netiesioginės valstybės atsakomybės fenomeno, paremto valstybės nesugebėjimu vykdyti tarptautinių įsipareigojimų. Šis pokytis itin svarbus kalbant apie kibernetines atakas. Anksčiau vyravęs kibernetinių atakų tapatinimas su kriminaliniais nusikaltimais, o ne su grėsme nacionaliniam saugumui, apriboja valstybes atsakomybę priskirti konkretiems subjektams, net ir žinant, koks mažai tikėtinas toks priskyrimas.

Kibernetinio nusikalstamumo ir kibernetinio saugumo klausimai turėtų būti sprendžiami remiantis 2001 m. pasirašyta ir 2004 m. įsigaliojusia Kibernetinių nusikaltimų konvencija (taip pat žinoma kaip "Budapešto Konvencija"), priimta Europos Tarybos. Dokumente valstybėms siūloma įtraukti kibernetinį nusikalstamumą į baudžiamuosius kodeksus ir ieškoti įrodymų, pagrindžiančių neteisėtą veiklą.[46] JAV yra vienintelė ne Europos valstybė, pasirašiusi susitarimą, tuo tarpu nei Rusija, nei Kinija, susitarimo pasirašyti nesutiko. Nepaisant to, jog susitarimas yra regioninio lygmens, jis yra reikšmingas dėl jį pasirašiusių valstybių vaidmens tarptautinėje sistemoje. Be to, ši konvencija įrodo, kad

[43] Ten pat, 261.
[44] Ten pat, 265.
[45] Ten pat, 265.
[46] Council of Europe, "Convention on Cybercrime", 2001. < https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561>

valstybėms svarbus kibernetinių atakų klausimas, galimas jų kriminalizavimas, priskyrimas ir valstybių pareiga išvengti, jog jos teritorija būtų naudojama nevalstybinių veikėjų, organizuojant kibernetines atakas prieš kitas valstybes. Taip pat konvencijoje pabrėžiama valstybių bendradarbiavimo svarba ir siekiamas rasti teisinis sutarimas kaip atgrasymo mechanizmas, bet kartu ir būdas priskirti atsakomybė dėl įvykusių atakų konkrečiai valstybei.[47]

Šios grėsmės įtraukiamos į regionines ar tarp-regionines sutartis ne tik Europoje, Azijoje (pvz. Azijos ir Ramiojo vandenyno regioninio bendradarbiavimo sutartis "National Computer Emergency Response Teams ("CERT") ir Computer Security Incident Response Teams ("CSIRTs"))[48], JAV ("Organization of American States"("OAS"), orientuota reaguoti į kibernetinius nusikaltimus regione).[49] Svarbu paminėti, kad Vakarų demokratijų ir Eurazijos bloko valstybių kibernetinės erdvės suvereniteto suvokimas ženkliai skiriasi. Atsižvelgiant į tai, 2011 m. Rusija, Kinija, Tadžikistanas ir Uzbekistanas Jungtinių Tautų Generalinei Asamblėjai pateikė kodekso "Tarptautinį kodeksą siekiant užtikrinti informacinį saugumą" ("International Code of Conduct for Information Security") projektą, kuris vetuotas JAV.[50] 2015 m., vadinamuoju post-Snowden laikotarpiu, Šanchajaus bendradarbiavimo organizacijos (ŠBO)[51] narės – Kinija, Rusija, Kazachstanas, Kirgizija, Tadžikistanas ir Uzbekistanas dar kartą JT Generalinei Asamblėjai pateikė patobulintą dokumento versiją. Tikslu ir toliau išlieka identifikuoti valstybių teises ir atsakomybes kibernetinėje erdvėje, skatinti konstruktyvų ir atsakingą elgesį, sustiprinti bendradarbiavimą kovojant su bendromis grėsmėmis ir iššūkiais kibernetinėje erdvėje, siekiant užtikrinti tarptautinę taiką ir saugią. Nors kodeksų turinys panašus, pastaroji versija labiau akcentuoja interneto erdvės valdymą ir

[47] Matthew J.Sklerov, "Solving the Dilemma of States Responses to Cyberattacks: a Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent", 2009, 6. <https://www.hsdl.org/?view&did=12115>

[48] Council for Security Cooperation in the Asia Pacific (CSCAP), "Ensuring A Safer Cyber Security Environment", Memo. No. 20, 2012. <http://www. cscap.org/uploads/docs/Memorandums/CSCAP%20Memorandum%20No%2020% 20--%20Ensuring%20a%20Safer%20Cyber%20Security%20Environmenet.pdf>

[49] Organization of American States, Secretariat of Legal Affairs, "Inter-American Cooperation Portal on Cyber-Crime". <http://www.oas.org/juridico/english/cyber.htm>

[50] United Nations General Assembly, A/66/150, 2011. <https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf>

[51] Šanchajaus bendradarbiavimo organizacija (ŠBO) įkurta 2001 m. birželio 15 d., keturioms Vidurio Azijos valstybėms (Kazachstanas, Kirgizija, Turkmėnija ir Tadžikistanas), Rusijai ir Kinijai Šanchajuje pasirašius sutartį, įsteigti naują regioninį darinį. Šiuo žingsniu siekiama įtvirtinti valstybių bendradarbiavimą netradicinių grėsmių akivaizdoje, bei kovoti su "trimis blogiais": terorizmu, separatizmu ir ekstremizmu, tačiau į savo darbotvarkę įtraukdama ir informacinį saugumą. McKune, Sarah, "An Analysis of the International Code of Conduct for Information Security", 2015.<https://citizenlab.org/2015/09/international-code-of-conduct/>

lygių teisių valstybėms užtikrinimą sprendžiant skaitmeninės politikos klausimus.[52] Abu dokumentai nesulaukė tarptautinio pripažinimo, tačiau neatmetama galimybės, kad dokumentuose pateikti pasiūlymai gali būti taikomi regioniniu lygiu.[53] Vienintelis dokumentas, su kurio principais sutiko ŠBO narė Kinija - 2013 m. birželį JT Vyriausybės ekspertų grupės (UN Group of Government Experts (GGE)) pristatytas susitarimas "Developments in the Fields of Information and Telecommunications in the context of International Security", kuriame patvirtinamas tarptautinės teisės taikymas kibernetinėje erdvėje. Vyriausybės Ekspertų Grupę sudaro šalių narių ekspertai, Generalinio Sekretoriaus pasirinkti peržiūrėti egzistuojančias ir potencialias kibernetines grėsmes ir galimus būdus jas spręsti. Kinija sutiko ne tik su bendruoju tarptautinės teisės taikymo kibernetinei erdvei principu, bet ir su specifinių aspektų, tame tarpe ir valstybės atsakomybės principo taikymu, bei JT Konvencijos punktu dėl jėgos panaudojimo ir ginkluotų konfliktų.[54]

Valstybės vis daugiau dėmesio skiria kibernetinių atakų problematikai, šis klausimas iškeltas ir JT Generalinėje Asamblėjoje. Generalinė Asamblėja pateikė pasiūlymus valstybėms kriminalizuoti kibernetines atakas ir tokiu būdu užkirsti kelią valstybės teritorijos naudojimą neteisėtiems veiksmas kibernetikoje atlikti. 2005 ir 2010 metais išryškinant pasitikėjimo didinimo būtinybę sukuriamas mandatas, ekspertų grupė, siekianti didinti informacinį ir kibernetinį saugumą, skaidrumą ir pasitikėjimą, mažinti valstybių pažeidžiamumą, kurti "taikią aplinką".[55] Taip pat asamblėja skatina valstybes bendradarbiauti tarpusavyje tiriant ir priskiriant atakas, persekiojant nusikaltėlius (jeigu yra sutarta). Visos JT Generalinės Asamblėjos deklaracijos kalba apie valstybės pareigą išvengti kibernetinių atakų visomis įmanomomis teisinėmis priemonėmis, kartu įtraukiant ir pareigas: griežtinti baudžiamuosius įstatymus, aktyviai tirti kiekvieną kibernetinį incidentą, persekioti pažeidėjus, skatinti puolusios ir nukentėjusiosios valstybių bendradarbiavimą tiriant nusikaltimą. Priskyrimas, pasak šalių narių, išlieka pagrindiniu iššūkiu, nes reikalingas techninis ir/arba teisinis priskyrimas, siekiant valstybės atsakomybės, pvz. kreipiantis į

[52] United Nations General Assembly, A/69/723, 2015. <https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf>

[53] Platesnė dokumentų analizė prieinama <https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html>

[54] Kimberly Hsu ir Craig Murray, "China and International Law in Cyberspace". U.S. – China Economic and Security Review Commission Staff Report, 2014, 3. <https://www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf>

[55] Detlev Wolter, "The UN Takes a Big Step Forward on Cybersecurity". Arms Control Association, 2013. <https://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity>

Saugumo Tarybą ir taikant Valstybių atsakomybės už tarptautinius neteisėtus aktus straipsnių projekte numatytas sąlygas.[56]

Kitas svarbus žingsnis 2013 m. buvo žengtas Jungtinėse Tautose, kur 15 šalių narių sutarimu nuspręsta pilnai taikyti tarptautinę teisę ir valstybių atsakomybė dėl valstybės veiksmų kibernetinėje erdvėje.[57] Visgi sprendimas dar nėra tapęs paprotine tarptautine teise ir vis dar nėra privalomas taikyti pagal viešąją tarptautinę teisę. Tais pat metais išleista Europos Sąjungos kibernetinio saugumo strategija "An Open, Safe and Secure Cyberspace"[58] ir su ja susiję direktyvos buvo reikšmingas kibernetinio saugumo užtikrinimo ES lygiu įsipareigojimams. Šiuo dokumentu siekta mažinti valstybių narių politinę fragmentaciją. Kitas žingsnis - 2013 m. Europos tinklų ir informacijos saugumo agentūros ("ENISA")[59] įsteigimas, kurios pagrindinis tikslas – koordinuoti atsaką į kibernetinio saugumo klausimus ir yra kaip platforma tarvyriausybiniam bendradarbiavimui ES.

Kaip ne kartą minėta, didžiausi sunkumai siekiant priskirti atsakomybę valstybei kyla norint identifikuoti kenkėjus, veikiančius kibernetinėje erdvėje. Galimi keli būdai, kaip, remiantis precedentu, būtų galima priskirti atsakomybę valstybei kibernetinėje erdvėje: efektyvios ir bendrosios kontrolės standartai. Valstybę laikant atsakinga už jos teritorijoje veikiančias paramilitarines organizacijas ir kitus nevyriausybinius veikėjus, galima kalbėti apie efektyvios kontrolės testo taikymą (t.y. veikėjai yra pilnai priklausomi nuo valstybės, taigi valstybė faktiškai vykdo ir koordinuoja operacijas).[60]

Ši sąvoka naudota Tarptautinio teisingumo teisme Nikaragvos byloje ir tinka kalbant apie nevalstybinius veikėjus ir paramilitarinį kontekstą. Jeigu efektyvios kontrolės testas būtų naudojamas kibernetikoje, tai reiškia, kad valstybės įsitraukimas būtų laikomas nepaneigiamu tik tokiu atveju, jeigu efektyvi kontrolė būtų neginčytina.[61] Prisimenant techninius iššūkius, su kuriais susiduriama siekiant identifikuoti kenkėjus, tokio standarto taikymas uždegtų žalią šviesą valstybės remiamoms kibernetinėms atakoms.

---

[56] Ten pat.
[57] U.N.G.A., Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security, 2013.
[58] European Commission, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", 2013. < http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf >
[59] European Network and Information Security Agency (ENISA), "National Cyber Security Strategies: Practical Guide on Development and Execution", 2012. <http://www.enisa.europa.eu/activities/ Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security- strategies-an-implementation-guide>
[60] Scott J. Shackelford, "State Responsibility for Cyber Attacks: Competing standards for a growing problem". Conference on Cyber Conflict, Estonia, 2010.
[61] Scott J.Shackelford ir Richard B.Andres, "State Responsibility for Cyber Attacks: Competing Standarts for a Growing Problem". Georgetown Journal of International Law, Vol.42, 2011.

Labiau sofistikuotose ir platesnio masto kibernetinėse atakose, esant informacijos trūkumui ar ją pakeitus, tai gali būti laikoma pakankamu faktoriumi pagrįsti valstybės kontrolės nebuvimui ir valstybės nepajėgumui. Apie bendrosios kontrolės testo taikymą, atsispindintį Tarptautinio baudžiamojo tribunolo buvusios Jugoslavijos respublikos Tadic byloje[62], galima kalbėti, kai valstybė organizuoja, koordinuoja ir remia nevyriausybinius veikėjus, vykdančius atakas. Tuo tarpu Tarptautinio teisingumo teismas naudoja siauresnį efektyvios kontrolės standartą, remdamasis Bosnijos Genocido byla, tačiau teisėjas Antonio Cassese, pirmasis Hagos Tribunolo prezidentas, reaguodamas į Bosnijos Genocido bylą teigė, kad keliami per aukšti ir nerealistiškai standartai įrodymams.[63] Atsižvelgiant į interneto specifiką ir anonimiškumo kibernetikoje aspektą, efektyvią kontrolę būtų labiau sunku įrodyti tyrimu, kas darytų priskyrimą remiantis efektyvia kontrole neįmanomu. Siekiant palengvinti priskyrimą, tarptautinė teisė turi būti lanksti ir pritaikoma kibernetinių atakų problematikai, taigi netgi ir bendrojo kontrolės testo standartų taikymas turi būti suvokiamas kaip būtinas tarptautinio saugumo užtikrinimo elementas, todėl taikomas laisviau.

Mažai taikytas ir nagrinėtas, tačiau pakankamai lankstus ir pritaikomas yra valstybės atsakomybės priskyrimo standartas, dar įvardijamas kaip vyriausybės sąmoningumo požiūris ("Government Awareness" approach). Jis remiasi precedentu, Irano įkaitų krize (Iran Hostages case), byloje apibrėžiama, kad valstybės piliečių veiksmai gali būti priskirti valstybei, jeigu jie buvo atliekami su valstybės žinia ir buvo valstybės palaikomi bei remiami. Irano byloje šis standartas atsispindėjo per valstybės organų paramą vykdant specifines operacijas.[64] Nors Teismui nepavyko rasti pakankamai įrodymų priskirti piliečių veiksmus valstybei, tačiau buvo pasiektas sutarimas, kad Irano vyriausybė yra neginčytinai kalta dėl 1961 m. Vienos Konvencijos dėl diplomatinių santykių ir 1963 m. Konvencijos dėl konsulinių santykių, siekiant apsaugoti JAV ambasadą ir jos darbuotojus įsipareigojimų pažeidimų.[65]

Nepaisant nepavykusio priskyrimo, Tarptautinio Teismo išdėstyti samprotavimai gali būti pritaikomi kibernetikoje dviem būdais. Pirmiausiai, valstybės galėtų būti laikomos atsakingomis už kibernetinėmis atakomis sukeltą žalą, jeigu valstybės piliečiai veikė

[62] Prosecutor v. Dusko Tadic, "Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction", IT-94-1-A, 1995. < http://www.refworld.org/cases,ICTY,47fdfb520.html>
[63] Caroline Tosh, "Genocide Acquittal Provokes Legal Debate", Institute of War and Peace Reporting, 2007. < https://iwpr.net/global-voices/genocide-acquittal-provokes-legal-debate>
[64] Scott J. Shackelford, "State Responsibility for Cyber Attacks: Competing standards for a growing problem". Conference on Cyber Conflict, Estonia, 2010, 203.
[65] Scott J.Shackelford ir Richard B.Andres, "State Responsibility for Cyber Attacks: Competing Standarts for a Growing Problem". Georgetown Journal of International Law, Vol.42, 2011, 989.

kompetentingų valdžios organų žinioje. Antra, jeigu nėra pakankamai įkalčių priskirti atsakomybę, kaip kad Irano bylos atveju, tuomet galima taikyti valstybės sąmoningumo lygio testą. Jeigu vyriausybė žinojo apie savo įsipareigojimus pagal tarptautinę teisę užkirsti kelią kibernetinei atakai ir nesilaikė šių įsipareigojimų, tuomet valstybė gali būti laikoma pažeidusia tarptautinę teisę. Daugelis valstybių, nepaisant trūkumų, linktų prie bendrojo kontrolės testo standartų taikymo. Abiem atvejais, tiek taikant bendrosios kontrolės, tiek vyriausybės sąmoningumo požiūrio, valstybės atsakomybės procesas supaprastėja, jeigu pavyksta rasti įrodymų dėl valstybės įsitraukimo.[66]

Vienas iš pagrindinių iššūkių, su kuriuo susiduria valstybės, nagrinėdamos neteisėtus veiksmus kibernetinėje erdvėje yra tarptautinės teisės pritaikomumas tokių atakų atveju. Didžioji dalis tarptautinių sutarčių ir normų buvo pasirašytų anksčiau ir nekito, kai tuo tarpu technologijos, kurias galima panaudoti kibernetikoje, žengė į priekį. Reaguojant į teisinių dokumentų, apibrėžiančių veiksmų kibernetinėje erdvėje traktavimą, trūkumą 2012 m. NATO Kibernetinės gynybos kompetencijos centras (NATO Cooperative Cyber Defence Center of Excellence) parengė dokumentą - „Talino vadovas dėl tarptautinės teisės, taikytinos kibernetiniams karams"[67] (toliau – Talino vadovas), kuriame kalbama apie plataus spektro su kibernetiniu saugumu susijusią problematiką, nuo valstybės atsakomybės iki atsako į atakas, nagrinėjamas tarptautinės teisės pritaikomumas kibernetiniam karui. Kaip teigiame dokumento įžangoje, tai nėra kibernetinio saugumo vadovas. Nepaisant to, jog skirtingos priemonėmis kibernetinėje erdvėje galima sukelti grėsmę valstybės saugumui, adekvačiam atsakui reikalingas valstybių bendradarbiavimas ir sutarimas dėl taikytinų priemonių. Vadove nėra aptariamos priemonės, kaip ir teisiniai jėgos panaudojimo ginkluotame konflikte aspektai, tačiau jis taikytinas tiek tarptautinių, tiek netarptautinių konfliktų atveju. Pirmiausiai todėl, kad tiek kibernetinės priemonės gali būti labai įvairaus pobūdžio: nuo serverių darbo trikdymo (DDos atakos), slaptos informacijos ieškojimo ir pasisavinimo, iki įrangos gadinimo. Lygiai taip pat atakos tikslas gali būti labai įvairus, nebūtinai orientuotas į išmatuojamą fizinę žalą, tačiau gali būti siekiama mažinti pasitikėjimą, skleisti propagandą ir kitaip netiesiogiai veikti valstybės gyventojus. Kaip pastebi ir Louise'as Arimatsu, kenkėjiškos programos nesukurtos taip, kad žudytų ar žalotų žmones, ir jos nebūtinai gadins ar naikins turtą.[68] Kinetinėmis priemonėmis padaryta žala retu atveju gali būti sulyginama su

[66] Ten pat, 989.
[67] Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013. <http://csef.ru/media/articles/3990/3990.pdf>
[68] L. Arimatsu, "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations". 4th International Conference on Cyber Conflict Proceedings, supra note 6, 2012, 97.

poveikiu, kokį sukelia kibernetinės atakos, tačiau tai nesumenkina problemos aktualumo.

Pirmasis vadovo skyrius apeliuoja į tarptautinį teisinį santykį tarp valstybės, kibernetinės infrastruktūros ir kibernetinių operacijų. Kibernetine infrastruktūra laikomi visi komunikaciniai, saugojimo ir skaičiavimo resursai, dėka kurių veikia sistema. Svarbūs suvereniteto ir valstybės kontrolės klausimai. Valstybės kontroliuojama kibernetinė infrastruktūra iš karto sukuria teises ir pareigas, taigi ir teisinę atsakomybę. Kibernetinė infrastruktūra yra teisiškai reguliuojama ir kontroliuojama valstybės, o teritorijos suverenumo principu remiantis kibernetinė infrastruktūra yra saugotina, nepaisant to ar ji tiesiogiai priklauso valstybei, privatiems ar individualias veikėjams, nepriklausomai nuo jos turėjimo priežasties.[69]

Kibernetinėmis operacijomis laikytini veiksmai, kur kibernetiniai pajėgumai panaudojami siekiant tikslo kibernetinėje erdvėje ar naudojantis kibernetine erdve. Remiantis tarptautine teise, valstybės yra atsakingos už operacijas, kurios yra atliekamos jų institucijų arba kitu atveju turi būti priskirtos remiantis valstybės atsakomybe. Vadove minima, kad nevalstybinių veikėjų veiksmai kibernetinėje erdvėje, esant tam tikroms sąlygoms (galima naudoti Healey skalę), taip pat gali būti priskirti valstybei (išskyrus valstybės nepajėgumą išvengti atakų, pvz. trūkstant techninių pajėgumų), kas apibrėžta 1 taisyklės 8 punkte.[70]

Daugiausiai diskusijų sulaukia ”kitų subjektų”, t.y. nevalstybinių veikėjų įsitraukimas. Vadovo kūrėjų manymu, jie taip pat laikytini valstybės dalimi. Pvz. CŽV būtų laikomi valstybės ginkluotųjų pajėgų dalimi, nors prastai tarptautinė humanitarinė teisė būtent valstybių vidaus teisei palieka apibrėžimą, kas yra „ginkluotosios pajėgos“. Talino vadove tokia išvada daroma remiantis valstybių atsakomybės principais, kadangi tokiais atvejais šie subjektai vykdo jiems priskirtas funkcijas, kurios paprastai priklauso kitoms institucijoms. Sudėtingiau, kai į jėgos naudotojų ratą patenka subjektai, kurių ryšys su valstybe ar jos institucijomis būna kitokio pobūdžio. Pavyzdžiui, pasitelktos privačios kompanijos ir kiti nevalstybiniai veikėjai arba individų grupės, pavieniai individai. Tarptautinėje teisėje yra mechanizmai, kuomet valstybė laikoma atsakinga ir už privačių asmenų veiksmus (pavyzdžiui, jeigu valstybė prisiima atsakomybę ar jeigu asmenys *de facto* veikė kaip valstybės institucija)[71], ta pačia linkme argumentuojama ir Talino vadove. Tokiu atveju, norėdami vienokio ar kitokio subjekto kibernetinio puolimo veiksmus priskirti valstybei,

[69] Tallinn Manual on the International Law Applicable to Cyber Warfare, 1 taisyklės 5 punktas, 25 psl.
[70] Ten pat, 1 taisyklės 8 punktas, 24 psl.
[71] Justinas Žilinskas, “Kibernetinių technologijų panaudojimo ginkluotose konfliktuose poveikis tarptautinei humanitarinei teisei”. Jurisprudencija, 20(3), 2013. <https://www.mruni.eu/upload/iblock/85d/JUR-13-20-3-17.pdf>

turėtume remtis anksčiau aptartais efektyvios kontrolė arba bendrosios kontrolės testais. Jeigu šių veikų valstybei priskirti nepavyksta, negalima konstatuoti tarptautinio konflikto, teisinės atsakomybės klausimas tampa negalimas.

Kad būtų užtikrintas valstybės neįsitraukimas, 5-oji Vadovo taisyklė skatina valstybes neleisti kibernetinės infrastruktūros, kuri vėliau gali būti panaudota neteisėtiems veiksmams prieš kitą valstybę, vystymo savo teritorijoje.[72] Ši taisyklė taikoma tiek valstybės valdomai kibernetinei infrastruktūrai, tiek kibernetinei infrastruktūrai, dislokuotai kitur, tačiau valstybė turi jos *de jure* ar *de facto* vykdomąją kontrolę. Taip pat ja apeliuojama į valstybės teritorinio suverenumo taisyklę, kuri įtvirtinta Tarptautinio Teisingumo Teismo Nikaragvos byloje "tarp nepriklausomų valstybių, pagarba teritorijos suverenumui yra tarptautinių santykių pagrindas".[73] Pagal tarptautinę teisę, iš valstybių reikalaujama imtis atitinkamų veiksmų, siekiant užtikrinti, kad ši teisė būtų saugoma. Taisyklė galioja ne tik kriminaliniams nusikaltimams prieš kitą valstybę, bet ir veiksmams, kurie implikuoja rimtą žalą arba turi potencialo tokią žalą sukelti (laiko perspektyvoje) žmonėms ar objektams, saugomiems remiantis valstybės teritoriniu suverenumu. Vienas esminių šios taisyklės elementų, jog kibernetinės operacijos žala aiškiai atskiriama nuo kinetinės - kibernetinių atakų sukelta žala neturi sukelti fizinės žalos objektams ar sužeidimų individams, pakankama žala laikytinas kibernetine ataka sukeltas neigiamas poveikis. Jeigu valstybė nesiima reikiamų veiksmų galimam poveikiui sustabdyti, nukentėjusi valstybė turi teisę kreiptis dėl tarptautinės teisės pažeidimo ir imtis proporcingo atsako, kuris gali apimti atsakomąsias priemones (įtvirtintas 9 taisyklėje) ar jėgos panaudojimą savigynos tikslais (13 taisyklė), kas gali peraugti į tarptautinį ginkluotą konfliktą, apibrėžtą 94 Vadovo taisykle.

Jurisdikcijos apsibrėžimas kalbant apie atsakomybės priskyrimą yra svarbus.[74] Laikytina, kad nepažeidžiant savo tarptautinių įsipareigojimų, valstybė pagal savo jurisdikciją yra atsakinga už: asmenis, užsiimančius kibernetine veikla jos teritorijoje; kibernetinę infrastruktūrą, esančią jos teritorijoje; eksteritorialumas[75] atsižvengiant į tarptautinę teisę.

Nekyla abejonių, kad Talino Vadovo įtvirtinta valstybės atsakomybės sąvoka yra viena tiksliausių sąvokų, tinkančių kibernetikos problematikai. Daugelyje anksčiau minėtų dokumentų atsakomybės klausimas keliamas, aptariamas, teikiami pasiūlymai, tačiau Vadove kalbama apie realią teisinę valstybės atsakomybę už kibernetinėje erdvėje įvykusius

[72] Tallinn Manual on the International Law Applicable to Cyber Warfare, 5 taisyklės 2 punktas, 33.
[73] Justinas Žilinskas, "Kibernetinių technologijų panaudojimo ginkluotose konfliktuose poveikis tarptautinei humanitarinei teisei". Jurisprudencija, 20(3), 2013.
[74] Tallinn Manual on the International Law Applicable to Cyber Warfare, 2 taisyklė, 27 psl.
[75] Eksteritorialumas- tam tikrų asmenų ir patalpų, esančių svetimos valstybės teritorijoje, nepriklausymas tos valstybės civilinei ir baudžiamajai jurisdikcijai. <http://www.lietuviuzodynas.lt/terminai/Eksteritorialumas>

incidentus. Valstybės neša tarptautinę teisinę atsakomybę už joms priskirtas kibernetines operacijas, kuriomis pažeidžiami tarptautiniai įsipareigojimai. Visi veiksmai ar siekio juos sustabdyti nebuvimas turi būti priskirti valstybei, o valstybė turi pilnai nešti atsakomybę už juos. Nors konceptas "valstybės institucijos", minimas Valstybių atsakomybės už tarptautinius neteisėtus aktus straipsnių projekte, į kurį referuojama Vadovo 6-oje taisyklėje, apibrėžiančioje valstybės atsakomybę yra platus, galimos kelios apibrėžimo variacijos. Siūloma laikyti, kad kiekvienas fizinis ir juridinis asmuo, kuris turį tokį statusą remiantis valstybės vidaus teisės aktais, būtų laikomas valstybės organu, nepaisant jo atliekamos funkcijos ir vietos hierarchijoje. Bet kuri neteisėta veika kibernetikoje, atlikta žvalgybos, kariuomenės, vidaus saugumo tarnybų, muitinės ar kitos valstybės agentūros, jai pažeidus tarptautinius teisinius įsipareigojimus, saistančius valstybę, automatiškai yra valstybės veiksmas.[76] Šiuo atveju netgi nėra svarbu, ar veiksmai buvo tiesiogiai koordinuoti ir vykdomi su valstybės instrukcijomis.

2017 m. pasirodęs Talino vadovas 2.0, papildyta 2013 m. dokumento versija, aptaria plataus tarptautinės teisės taikymo galimybes kibernetiniams konfliktams. Analizėje apžvelgiamas ir bendrosios tarptautinės teisės principų taikymas, kaip suverenitetas ir valstybių jurisdikcijos klausimai. Daugiau dėmesio skiriama valstybių atsakomybės klausimui, teisiniams priskyrimo aspektams, įtraukiant žmogaus teises, oro, jūrų, kosmoso teisę, diplomatinę ir konsulinę teisę, nagrinėjant kibernetinėje erdvėje kylančių atakų kontekstą. Pirminiame Vadovo leidime dėmesys skiriamas kibernetinėms atakoms ir valstybėms, kurios pažeidė jėgos panaudojimo draudimą ar pasinaudojo savigynos teise, antrajame leidime - kibernetiniams incidentams, su kuriais valstybės susiduria kasdien. Šiuo dokumentu siekiama užtikrinti, kad kibernetinėje erdvėje vykstantys veiksmai nepapultų į "teisinį vakuumą", o valstybėms būtų priminta apie jų tarptautine teise numatytas teises ir pareigas užtikrinti, kad neteisėti veiksmai sulauktų atsako.[77] Kaip taikliai pastebi Pierluigi Paganini, Europos Sąjungos tinklų ir informacijos saugumo agentūros (ENISA), narys, Talino vadove 2.0 analizuojamos veiklos kibernetinėje erdvėje, kurios patenka į modernaus informacinio karo kategoriją. Netgi dokumentų antraštės, lyginant su pirmuoju leidimu kito, nuo "taikoma informaciniam karui" (Talino vadovas) į "taikoma kibernetinėms operacijoms" (Talino vadovas 2.0). Siūloma į veiklą kibernetinėje erdvėje žiūrėti plačiau, siekiant rasti būdus, kaip egzistuojanti tarptautinė teisė galėtų būti pritaikoma tokiems konfliktams ir jų

[76] Tallinn Manual on the International Law Applicable to Cyber Warfare, 6 taisyklė, 35 psl.
[77] CCDCOE, "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", NATO Cooperative Cyber Defence Centre of Excellence, Estonia, 2017. <https://ccdcoe.org/sites/default/files/documents/CCDCOE_Tallinn_Manual_Onepager_web.pdf>

sprendimui. Akcentuojama atsakomybės valstybėms priskyrimo svarba, kas įgalintų aktyvią gynybą arba netgi galimybę imtis kibernetinio atsako.[78]

Nepaisant pastangų, priskyrimo klausimas vis dar yra "pilkoji zona", teisinės sankcijos prieš agresorių negali būti taikomos, jeigu jis nėra aiškiai žinomas. Michael Schmitto, abiejų Talino vadovų rengimo iniciatoriaus, tarptautinės humanitarinės teisės eksperto teigimu, priskyrimas nėra tik techninės detalės, priskyrimas grindžiamas ne tik technologijomis, bet remiasi eile rodiklių: žvalgybos informacija, geopolitika. Svarbiausias priskyrimo elementas, turint pakankamai duomenų apie pažeidėją - valstybės pozicija ir politinė valia, jeigu valstybės sutinka, kad valstybė privalo atsakyti už neteisėtus veiksmus kibernetinėje erdvėje, Talino vadovas gali būti taikomas, siekiant rasti teisinį būdą į tokius veiksmus reaguoti.[79]

Tarptautinio susidomėjimo Talino vadovas ir Talino vadovas 2.0 sulaukė, nes pateikia teisinę poziciją, tačiau valstybės nėra priverstos deklaruoti savo pozicijų.[80] Abi versijos yra tik rekomendacinio pobūdžio, t.y. neturi jokio teisinio autoriteto, todėl ten apibrėžtų normų laikyti neprivaloma, o nesilaikant jokia teisinė atsakomybė netaikoma. Nepaisant to, dokumentai sulaukė didelio ekspertų susidomėjimo ir naudojami ieškant teisinių atsakymų į su kibernetine erdve susijusius klausimus. J. Healey pateikta ir ankstesniame skyriuje pristatyta schema valstybės atsakomybei nustatyti, taikoma kartu su Thomas Rido ir Ben Buchanano Q modeliu tolimesniam tyrimui, gali būti patogus metodologinis įrankis, atveriantis galimybę pilnai priskirti atsakomybę valstybei, nepaisant įrodymų trūkumo, kylančio dėl techninių parametrų, taip pat įtraukiant ir politinio elito, priimančio sprendimus dėl politinės atsakomybės priskyrimo, svarbą.

Valstybių atsakomybės kibernetikoje klausimas nėra nauja tema, tačiau tarptautinėje teisėje vystoma lėčiau, nei technologijos, kuriomis naudojasi kibernetinių ataką organizatoriai. Netgi išanalizavus nemažą kiekį teisinių dokumentų, tarptautinių, regioninių ir tarp-regioninių sutarčių, konvencijų, viršnacionalinių organizacijų diskusijų bei kitų tiesiogiai į atsakomybės priskyrimą kibernetinių atakų atveju orientuotų dokumentų, lieka neaišku, kodėl diskusijos, idėjos ir sutarimai taip ir nepasiekia tarptautinės bendruomenės, netampa visuotinai taikytina ir nekvestionuotina norma. Lieka neaišku, kas stabdo precedentų iškėlimą

[78] Pierluigi Paganini, "NATO presents the Tallinn Manual 2.0 on International Law Applicable to cyberspace. Security Affairs, 2017. <http://securityaffairs.co/wordpress/56004/cyber-warfare-2/nato-tallinn-manual-2-0.html> [Žiūrėta 2017 04 19]

[79] Kevin Townsend, "NATO Published Tallinn Manual 2.0 on International Law Applicable to Cyber Ops". Security Week, 2017. <http://www.securityweek.com/nato-publishes-tallinn-manual-20-international-law-applicable-cyber-ops> [Žiūrėta 2017 04 19]

[80] Ten pat.

į tarptautinių organizacijų lygmenį, atsakomybės valstybės pripažinimą ir realių sankcijų taikymą. Siekiant atsakyti į šiuos klausimus, ir pastebėji kaip galima pritaikyti egzistuojančią teisinė bazę ir J. Healey pateiktą atsakomybės priskyrimo valstybėms schemą įvykusiems precedentams, atvejo studijai pasirinktas JAV šnipinėjimas (2006-2013 m. laikotarpiu), dėl kurio kalta įvardyjama Kinijos vyriausybė. Atvejis įdomus, nes leidžia nagrinėti ne pavienį incidentą, o kibernetinių atakų virtinę, be to, tai pirmas toks atvejis, kai kaltininkas, šiuo atveju Kinija, 2013 m. oficialioje Pentagono metinėje atsakaitoje įvardyjama kalta dėl neteisėtų veiksmų kibernetinėje erdvėje.

3. Atvejo studija: J. Healey valstybės įsitraukimo schemos taikymas JAV kibernetinio šnipinėjimo priskyrimui Kinijos vyriausybei

2016 metų birželį saugumo kompanija Rapid7[81] sudarė didžiausią kibernetinį pažeidžiamumą turinčių valstybių sąrašą. Dėl nesaugių tinklų pažeidžiamiausia valstybe laikoma Belgija, penktoji vieta tenka Kinija, po jos Honkongui, JAV užima keturioliktąją vietą.[82] Nepaisant to, būtent didžiosios galingos valstybės kaip JAV, Kinija, Vokietija ir Didžioji Britanija patiria daugiausiai įvairaus lygio kibernetinių incidentų.[83] 2012-2016 m. duomenis, 41% pasaulio kibernetinių atakų kyla iš Kinijos, 10% priskiriama JAV, 4,7% kilmės šalis yra Turkija.[84] Nors ekspertams pavyksta nustatyti atakų kilmės šalį, praktikos priskiriant atsakomybę už realias atakas valstybei trūksta.

Kibernetinių atakų aktyvumas itin išaugo 2006-2007m. laikotarpiu, 2010 m. kovą NATO ir EU paskelbė apie suaktyvėjusias atakas iš Rusijos ir Kinijos.[85] Atvejis analizei pasirinktas neatsitiktinai, tik kelios valstybės – Rusija, Kinija, Izraelis, Prancūzija, JAV ir JK turi labiausiai pažengusias kibernetines technologijas, žinių ir pajėgumų panaudoti

[81] National Exposure Index, <https://information.rapid7.com/national-exposure-index.html> [Žiūrėta 2017 04 28]
[82] James Titcomb, "Mapped: The countries most vulnerable to cyber-attacks", The Telegraph, 2016. <http://www.telegraph.co.uk/technology/2016/06/10/mapped-the-countries-most-vulnerable-to-cyber-attacks/> [Žiūrėta 2017 04 28]
[83] Top 20 Countries Found to Have the most Cybercrime <https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/> [Žiūrėta 2017 04 28]
[84] Top 10 Countries Where Cyber Attacks Originate, Government Technology, 2013. <http://www.govtech.com/security/204318661.html>; [Žiūrėta 2017 04 28]Top 10 Countries with Most Hackers in the World, Cyware, 2016. <https://cyware.com/news/top-10-countries-with-most-hackers-in-the-world-42e1c94e> [Žiūrėta 2017 04 28]
[85] The Cyberterrorism Project, 2010. <http://www.cyberterrorism-project.org/cyberterrorism-report/> [Žiūrėta 2017 04 29]

kibernetinę ataką, galinčią padaryti rimtą ilgalaikę žalą kitoms valstybėms, todėl yra realiausiai numanomos valstybės, kurios pačios ar remdamos nevyriausybinius veikėjus galėtų vykdyti įvairaus masto kibernetines atakas prieš kitas valstybes. Šios valstybės yra įtraukę kibernetinius ginklus į savo puolamosios ginkluotės arsenalą šalia kinetinių ginklų, turi patirties ir žinių apie kibernetiką kaip mokslą, patirties planuojant, organizuojant ir užkardant kibernetines atakas. [86]

Pirmieji rimti incidentas, susiję su Kinija, užfiksuoti dar 2006 m. rugpjūtį. Vyresnysis JAV karinių oro pajėgų karininkas pranešė, kad Kinija persisiuntė 10–20 terabaitų duomenų iš NIPRNet (neįslaptinto karinio tinklo).[87] Gruodžio mėnesį pripažinta, kad Kinijos programišiai yra atsakingi už JAV Bendruomenės rūmų kompiuterių atjungimą.[88] Kinijos veikla kibernetinėje erdvėje kelia problemų ir kitoms valstybėms: Vokietijai, JK[89], Prancūzijai[90]. Nuolat pasikartojantys aktyvūs Kinijos veiksmai kibernetinėje erdvėje tęsiasi metų metus, dauguma jų nukreipti į JAV karinį ir gynybos sektorius. 2013 m. gegužę pranešta, kad Kinijos programišiai įsilaužė į JAV gynybos sistemas ir pasisavino informaciją apie JAV karines technologijas. Tarp neteisėtai pasisavintų programų buvo informacija apie ginklų programas, tame tarpe ir Patriot raketinę sistemą, F–35 Joint Strike Fighter, kurią Australija perka iš JAV, Osprey tipo lėktuvą, JAV kovinį laivą, JAV laivyne naudojamas balistines raketas Aegis ir Black Hawk malūnsparnį.[91] Obamos išplatintame pranešime teigiama, kad Kinijos pagrindu brautis į JAV informacines sistemas gali būti kariniai

---

[86] James A.Lewis, "The "Korean" Cyber Attacks and Their Implications on Cyber Conflict". Center of Strategic and International Studies, 2009, 7. <https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf>

[87] Paul Rosenzweig, "Significant Cyber Attacks on Federal Systems – 2004-present", Lawfare, 2012. <https://www.lawfareblog.com/significant-cyber-attacks-federal-systems-2004-present> [Žiūrėta 2017 04 29]

[88] Ten pat.

[89] 2007 rugsėjis, pranešama, kad Vokietija, JK, Prancūzija ir JAV nukentėjo nuo neįvardytos Kinijos programišių grupuotės. Larry Greenemeier, "China's Cyber Attacks Signal New Battelfield Is Online", Scientific American, 2007. <https://www.scientificamerican.com/article/chinas-cyber-attacks-sign/> [Žiūrėta 2017 04 29]

[90] 2007 m. rugsėjis, Prancūzijos gynybos generalinis sekretorius Francis Delon pareiškė, kad į Prancūzijos informacines sistemas yra infiltruotos Kinijos nusikaltėlių grupuotės. John Leyden, "France blames China for hack attack". The Register, 2007. <https://www.theregister.co.uk/2007/09/12/french_cyberattacks/> [Žiūrėta 2017 04 29]

[91] Adam Segal, "Shaming Chinese hackers won't work because cyber-espionage is here to stay. The Guardian, 2013. <https://www.theguardian.com/commentisfree/2013/may/30/china-hacking-cyber-espionage-obama> [Žiūrėta 2017 04 29]; Ellen Nakashima, "Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies". The Washington Post, 2013. <https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html?utm_term=.5c8984050e80>; [Žiūrėta 2017 04 29]; Paul Rosenzweig, "Significant Cyber Attacks on Federal Systems – 2004-present".

pajėgumai, kurie galėtų būti panaudojami krizės metu, siekiant įgyti strateginį pranašumą. Po oficialaus pranešimo, Kinijos užsienio reikalų ministerijos atstovas Hua Chunying pareiškimą sukritikavo, pabrėždamas Kinijos norą užmegzti konstruktyvų dialogą su JAV, siekiant užtikrinti interneto tinkle saugumą.[92]

Akivaizdu, kad kibernetinėmis atakomis siekiama rinkti JAV žvalgybos, diplomatinio korpuso, ekonomikos ir gynybos sektorių informaciją, kurią Kinija galėtų pasinaudoti kuriant savo gynybos programą. Pateiktas pavyzdys yra pirmas toks atvejis, kai Pentagonas 2013 m. metinėje ataskaitoje tiesiogiai susiejo įvykius su Pekino vyriausybe.[93] Remiantis pranešimu, daugiau nei 90% JAV patiriamo kibernetinio šnipinėjimo kilmės šalis yra Kinija. Pentagono teigimu, Kinija, investuodama į JAV technologijų kompanijas, siekia tobulinti savo karines technologijas. Taip pat atkreipiamas dėmesys, jog Kinija aktyviai siekia tikslingai išnaudoti užsienio investicijas, skatina tarptautinius mainus, siekia pritraukti svetur patirties įgijusius studentus ir mokslininkus, valstybė remia industrinį ir techninį šnipinėjimą, siekiant pagerinti technines žinias, skatinti tyrimus apie naujas karines technologijas.[94] JAV Gynybos departamento išplatintame pranešime teigiama, kad Kinijos įsitraukimą galima pagrįsti, nes "įgūdžiai, reikalingi šioms invazijoms yra panašūs į tuos, kurie būtini kompiuterinių tinklų atakoms".[95] Abejonių neliko po JAV kibernetinio saugumo užtikrinimo firmos Mandiant 2013 m. pranešimo.[96] Firma susiejo vienos iš pažangiausių kompiuterių įsilaužėlių grupių veiklą su Kinijos vyriausybe. Kaip teigiama Mandiant[97] detaliame 60 lapų pranešime, grupė, įsikūrusi netoli Šanchajaus, ilgą laikė vykdė plataus masto kibernetinį šnipinėjimą. Kaltininkas nustatytas pavykus atsekti keturis tinklus, esančius netoli Šanchajaus, nes kai kurios kibernetinės operacijos buvo vykdomos iš lokacijos, kur įsikūrusi slapta Kinijos karinė divizija (žinoma kaip Unit 61398). Kompanijos teigimu, atakų mastai (platus atakuojamų organizacijų spektras) ir trukmė leidžia daryti prielaidas, apie Kinijos įsitraukimą į atakas ir

[92] David E.Sanger, "U.S. Blames China's Military Directly for Cyberattacks". The New York Times, 2013. <http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html> [Žiūrėta 2017 04 30]
[93] Jonathan Marcus, "US accuses China government and military of cyber-spying". BBC News, 2013. <http://www.bbc.com/news/world-asia-china-22430224> [Žiūrėta 2017 04 30]
[94] David E.Sanger, "U.S. Blames China's Military Directly for Cyberattacks". The New York Times, 2013.
[95] Jonathan Marcus, "US accuses China government and military of cyber-spying". BBC News, 2013.
[96] Pranešimas prieinamas registruotiems vartotojas, FireEye, "Threat Intelligence Report", <https://www.fireeye.com/current-threats/threat-intelligence-reports.html>, U.S. House Energy and Commerce Committee, "Hearing on Cyber Espionage and the Theft of U.S. Intellectual Property and Technology", testimony of James Lewis, 2013 birželio 9 d.
[97] Mandiant, privati kibernetinio saugumo kompanija, įsikūrusi 2004 m. Jos pagrindinė atsakomybė - padėti nustatyti ir reaguoti į kibernetines grėsmes, šiai kompanijai pavyko nustatyti įsilaužėlių grupę, sistemingai vagiančią informaciją iš mažiausiai 141 organizacijos pasauliniu mastu nuo 2006 m. Company Overview of Mandiant Corporation, 2017.
<https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=13634745>

paramą jas vykdančiai grupuotei.[98] Taip pat teigiama, jog rasta duomenų apie "China Telecom" specialias didelės spartos "fiber optic" linijas, nukreiptas į šias būstines, prisidengiant nacionalinės gynybos poreikiais.[99] Franko Gaffney, Saugumo politikos centro (Center of Security Policy) įkūrėjas taip pat patvirtino, kad FTB turi duomenų apie pasikartojančias kibernetines atakas prieš JAV kompanijas. Nors programišiai nebuvo įvardyti, tos pačios grupės asmenų neleistini veiksmai kibernetinėje erdvėje stebimi nuo 2011 m. Privačios saugumo bendrovės pirmuosius įsilaužimus pastebėjo 2008 m., programišiai buvo bene pirmieji sukūrę ir pradėję naudoti APT (Advanced Persistent Threat) techniką.[100] Lyg patvirtindama kaltinimus, programišių grupė, atsakinga už minėtą atakų seriją ir atakas prieš vieną didžiųjų informacinių portalų The New York Times[101] 2006-2013 m. laikotarpiu, po paviešintų atakų ir pradėto tyrimo, keliems mėnesiams nurimo, tačiau, pasak JAV vyriausybės atstovų ir Mandiant, grįžo prie pirminės veiklos po trijų mėnesių.[102]

Kitas svarbus faktas, leidžiantis abejoji Kinijos veiksmų ir retorikos patikimumu – išlaidų gynybai slėpimas. Pentagono pranešime analizuojamas Kinijos progresas modernizuojant kariuomenę. Pranešime pastebima,[103] kad skaidrumo trūkumas pateikiant skaičius apie karinius pajėgumus kelia įtampą regione. 2012 m. kovą Kinija skelbė, kad jos išlaidos karybai siekė 114 milijardų JAV dolerių ir išaugo 10.4%. Tuo tarpu Pentagono skaičiavimais ir duomenimis, Kinijos išlaidos karybos reikmėms 2012 m. buvo gerokai didesnės ir siekė tarp 135 ir 215 milijardai JAV dolerių.[104]

Kinijos teigimu, JAV pranešimai apie Kinijos veiklą kibernetinėje erdvėje neatitinka tikrovės.[105] Šalies atstovai praneša, kad būtent Kinija yra dažniausiai kibernetines atakas patirianti valstybės, didžioji dalis jų vykdomos iš JAV teritorijos. Klaidingais pranešimais

---

[98] Charles Riley, "Report: Chinese military engaged in "extensive cyber espionage campaign". CNN, 2013. <http://money.cnn.com/2013/02/19/technology/china-military-cybercrime/index.html?iid=EL> [Žiūrėta 2017 04 30]

[99] William Wan ir Ellen Nakashima, "Report ties cyberattacks on U.S. computers to Chinese military". The Washington Post, 2013. <https://www.washingtonpost.com/world/report-ties-100-plus-cyber-attacks-on-us-computers-to-chinese-military/2013/02/19/2700228e-7a6a-11e2-9a75-dab0201670da_story.html?utm_term=.7ca5d99a0a25> [Žiūrėta 2017 04 30]

[100] Cyber Attacks From China Are Bleeding the U.S., 2016. <https://www.centerforsecuritypolicy.org/2016/05/17/cyber-attacks-from-china-are-bleeding-the-u-s/> [Žiūrėta 2017 04 30]

[101] Nicole Perlroth, "Hackers in China Attacked The Times for Last 4 Months". The New York Times, 2013. <http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html> [Žiūrėta 2017 05 01]

[102] Adam Segal, "Shaming Chinese hackers won't work because cyber-espionage is here to stay. The Guardian, 2013.

[103] Pranešimo nuoroda neprieinama, remiamasi http://www.bbc.com/news/world-asia-china-22430224 informacija.

[104] Ten pat.

[105] Jacob Davidson, "China Accuses U.S. of Hypocrisy on Cyberattacks". Time, 2013. <http://world.time.com/2013/07/01/china-accuses-u-s-of-hypocrisy-on-cyberattacks/> [Žiūrėta 2017 05 01]

JAV siekia diskredituoti, sumažinti Kinijos patikimumą tarptautinės bendruomenės akyse ir nukreipti dėmesį nuo neteisėtų savo pačios veiksmų. Atsižvelgiant į tai, kad B. Obamos įspėjimai Kinijos prezidentui Xi, jog Kinijos šnipinėjimas ves link daug griežtesnių politinių sprendimų kaip sankcijos firmoms, kurios pelnosi iš neteisėtai gautos informacijos, platesnio masto apribojimai patenkant į JAV rinką, jau nekalbant apie abipusio pasitikėjimo nebūvimą, nėra veiksmingi, būtinas galutinis sprendimas atsakomybės priskyrime.

Kinija yra puikiai pasirengusi ne tik organizuoti, bet ir atremti kibernetines atakas. Santykinai savarankiška infrastruktūra daro Kiniją mažiau pažeidžiamą, tačiau šie teigiami pokyčiai ateina tik su ekonomikos modernizacija, Kinijos ekspertus vis dar neramina industrinės kontrolės sistemos pažeidžiamumas.[106] Atsižvelgiant į tai, jog valstybė kategoriškai neigia neteisėtus veiksmus prieš JAV kibernetinėje erdvėje, bei turimus pajėgumus ir žinias, įdomu ko valstybė imasi, jog būtų išvengiama atakų iš jos teritorijos:

- 2011 m. Rusijos, Kinijos, Tadžikistano ir Uzbekistano Jungtinių Tautų Generalinei Asamblėjai pateiktas kodekso "Tarptautinį kodeksą siekiant užtikrinti informacinį saugumą" projektas, vetuotas JAV pasisakant prieš. Nors valstybės pabrėžia suvereniteto ir teritorinio integralumo[107] svarbą bei primena apie valstybės teisę ir pareigą užtikrinti, kad jos informacinė erdvė ir infrastruktūra nebūtų naudojama neleistiniems veiksmas kibernetinėje erdvėje: atakoms, trikdžiams, diversijai,[108][109] pati Kinija pateiktų siūlymų nesilaiko.

- 2015 m. Šanchajaus bendradarbiavimo organizacijos narių dar kartą JT Generalinei Asamblėjai pateiktas patobulintas kodekso projektas. ŠBO valstybėms kodeksas manomai yra būdas iš naujo peržvelgti žmogaus teisių taikymo klausimus, išplėsti suvereniteto ir teritorinio integralumo kibernetinėje erdvėje sąvokas.[110] Abu dokumentai nesulaukė tarptautinio pripažinimo, tarptautinė bendruomenė nesutiko nei su JT kaip taisyklių priėmimo ir interneto priežiūros institucijos įtvirtinimu, nei su sąvokų, tokių kaip "kibernetinės erdvės suverenitetas", apibrėžimu.

- Kinijos atsisakymas prisijungti prie Budapešto Konvencijos dėl nusikaltimų kibernetinėje erdvėje parodo valstybės laikyseną tarptautinių susitarimų atžvilgiu. Tuo tarpu

---

[106] Adam Segal, "Shaming Chinese hackers won't work because cyber-espionage is here to stay. The Guardian, 2013.

[107] <"...pagarba suverenitetui, teritoriniam integralumui ir politinei visų valstybių nepriklausomybei> United Nations General Assembly, A/66/150, 2011, 4.

[108] <"Pakartotinai įtvirtinti valstybės teises ir atsakomybes, apsaugoti, laikantis atitinkamų teisės aktų ir įstatymų, jų informacinę erdvę ir kritinę infrastruktūrą nuo grėsmių, trikdžių, atakų, sabotažo."> United Nations General Assembly, A/66/150, 2011, 4.

[109] United Nations General Assembly, A/66/150, 2011. <https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf>

[110] Sarah McKune, "An Analysis of the International Code of Conduct for Information Security", 2015. <https://citizenlab.org/2015/09/international-code-of-conduct/> [Žiūrėta 2017 05 03]

JAV Konvenciją pasirašė 2006 m. ir reiškia stiprų palaikymą jos suformuotiems principams. Vienoje iš diskusijų tarp JAV mokslinio instituto Center for Strategic and International Studies (CSIS) ir Kinijos valstybinio mokslinio centro China Institutes of Contemporary International Relations (CICIR) 2012 m., pastarasis pareiškė nepritarimą dėl Konvencijoje minimo tarpvalstybinio įrodymų rinkimo siekiant pradėti baudžiamąjį persekiojimą dėl nusikaltimų kibernetinėje erdvėje, kas pažeistų valstybės suverenitetą, kaip jį suvokia Kinija.[111]

- Vienintelis sutarimas, kurį pavyko pasiekit, nepaisant esminių skirtumų dėl kibernetinės erdvės apibrėžimo, siejantis JAV ir Kiniją paskatintas JT. 2013 m. birželį JT Vyriausybės ekspertų grupė, kuriai priklauso ir Kinija, pasiekė susitarimą ir pristatė "Developments in the Fields of Information and Telecommunications in the context of International Security", kuriame patvirtinamas tarptautinės teisės taikymas kibernetinėje erdvėje. Kinija sutiko ne tik su bendruoju tarptautinės teisės taikymo kibernetinei erdvei principu, bet ir su specifinių aspektų, tame tarpe ir valstybės atsakomybės principo taikymu, bei JT Konvencijos punktų dėl jėgos panaudojimo ir ginkluotų konfliktų.[112]

Kaip anksčiau minėta, Kinija kibernetinės erdvės suverenitetą apibrėžia ir traktuoja kitaip nei JAV ar Vakarų demokratijos. Kinija siūlo "skaitmeninį" arba "internetinį" suverenitetą apibrėžti ir traktuoti kaip valstybių kontroliuojamą erdvę, kuriai taikoma vidaus teisė. Oficiali Kinijos užsienio reikalų ministerijos pozicija, jog suvereniteto kibernetinėje erdvėje principas apima šiuos veiksnius:

- valstybės jurisdikcijai priklauso kibernetinė infrastruktūra (ICT Information and Communication Technologies) ir veiksmai, kylantys iš jos teritorijos;
- nacionalinės vyriausybės turi teisę priimant viešąją politiką dėl veiklos kibernetinėje erdvėje (originaliame tekste naudojamas terminas "internete"), atsižvelgiant į nacionalinius poreikius;

[111] Kimberly Hsu ir Craig Murray, "China and International Law in Cyberspace". U.S. – China Economic and Security Review Commision Staff Report, 2014, 3. <https://www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf> [Žiūrėta 2017 05 03]

[112] Ten pat.

- jokia valstybė neturi teisės panaudoti kibernetinės erdvės ("interneto"), kišantis į kitos valstybės vidaus klausimus ar siekiant pakenkti kitos valstybės interesams.[113]

Atsižvelgiant į Kinijos kibernetinės erdvės apibrėžimą nenuostabu, jog valstybei nerūpi tarptautinės bendruomenės bei B. Obamos taikytas "įvardyk ir sugėdyk" ("naming and shaming") metodas, ją stebina neleistinos veiklos kibernetinėje erdvėje viešinimas tarptautiniu mastu bei galimų sankcijų taikymas. Žvelgiant į valstybės profilį (autoritarinis valdymas ir spaudos kontrolė), valstybė laikosi į valstybės vidų orientuotos politikos (state-centric orientation) kibernetinio saugumo klausimu, priešingai nei Vakarų demokratijos. Šaltiniai, kurias remiantis galima atlikti analizę apie Kinijos vidaus reikalus susiskirstę į autoritarinius (Užsienio reikalų ministerijų atstovų ir kitų valdžios pareigūnų pranešimai, apsiribojantys labai lakoniška informacija), dalinai arba ex-autoritarinius bei ne autoritarinius. Tiek autoritariniai, tiek vadinamieji neautoritariniai šaltiniai, o ypač valdžios bei karinės institucijos, kibernetinę erdvę apibrėžia kaip netradicinį, tačiau kritinį nacionalinio saugumo klausimą. Nors deklaruojama, jog Kinijos interneto kontrole siekiama užtikrinti piliečių kibernetinės erdvės "tyrumą", palaikant žodžio laisvę ir laisvą informacijos judėjimą internete, buvęs užsienio reikalų ministras Yang Jiechi pripažino, kad pasaulyje egzistuoja skirtingos socialinės sistemos, o atsižvelgiant į tai, Kinija, remdamasi vidaus teise ir siekdama kas geriausia jos interesui, turi užsiimti "reguliaciniu darbu".[114] Nepaisant apribojimų, Kinijos vyriausybė sutinka, kad kibernetinio saugumas yra globali problema, kelianti grėsmę nacionaliniam saugumui, ekonominiam vystymuisi, tuo tarpų ypač karinio sektoriaus atstovai linkę pabrėžti, kad nusikaltimai kibernetinėje erdvėje kelia grėsmę valstybės suverenitetui, taip pat ir valstybės gebėjimui palaikyti tvarką, socialinį stabilumą, apsaugoti tautą nuo vidinių ir išorinių neramumų (implikacija į Kinijos Komunistų Partijos siekius). Nors 2011 ir 2015 m. siūlymuose JT Generalinei Asamblėjai užsimenama apie būtinybę tarptautinei bendruomenei vieningai užtikrinti taisykles, normas ir struktūrą kaip kiekviena valstybė individualiai užtikrintų kad šie procesai ir mechanizmai veiktų, Kinijos ir sąjungininkių pasiūlymams nepritarta dėl pernelyg politizuotų ir ideologizuotų tikslų. Tiek JAV, tiek Vakarų visuomenės nepritarė Kinijos intencijoms tarptautiniais įsipareigojimais

[113] Ministry of Foreign Affairs of the People's Republic of China, Address by Vice Foreign Minister Li Baodong at the Opening Ceremony of the International Workshop on Information and Cyber Security, 2014 m. birželio 5 d. <thttp://www.fmprc.gov.cn /mfa_eng/wjbxw/t1162458.shtml>
[114] Michael D. Swaine, "Chinese Views on Cybersecurity in Foreign Relations". China Leadership Monitor, no. 42. <http://www.hoover.org/sites/default/files/uploads/documents/CLM42MS.pdf>

įtvirtinti "kibernetinio suvereniteto" koncepciją, kokią ją mato Kinija ir sąjungininkės, ir įtvirtinti JT kaip taisyklių priėmimo ir interneto priežiūros instituciją.[115]

Kinijos vaidmuo JAV kibernetinėje erdvėje išskirtinis ir patvirtintas daugelio precedentų, jos kaltė garsiai įvardijama. Siekiant aptikrinti ar J. Healey pristatytas teorinis modelis (valstybės įsitraukimo schema) yra taikytinas praktikoje, Kinijos veiksmai bus vertinami remiantis teorinėje dalyje pateikta skale. Žemiau esančioje lentelėje + ženklu žymima kategorija, kuri Kinijos atvejui tinka, remiantis aukščiau atlikta pirminių ir antrinių šaltinių duomenų analize. Kaip minėta anksčiau, naudojama lentelė su pagalbos (ar valstybė turi žinių apie galimą pasiruošimą atakai iš jos teritorijos, kibernetinės infrastruktūros egzistavimą ir vystymą) ir diplomatijos (ar egzistuoja dvišaliai ar daugiašaliai susitarimai, teisinė bazė, draudžianti kibernetinius nusikaltimus), tačiau atsisakant gynybos elemento, kadangi pirminis darbo tikslas yra rasti sąlygas atsakomybei priskirti. Atsižvelgiant į Kinijos laikyseną priimant teisinį sutarimą dėl kibernetinių atakų traktavimo ir kibernetinės erdvės suvereniteto įteisinimo, "diplomatijos" skiltis faktiškai neegzistuoja, nepaisant nesėkmingų bandymų Jungtinėse Tautose. Pasirinkta "diplomatija" langelius žymėti "-" ženklu tik ten, kur valstybės įsitraukimas, remiantis įrodymas, yra neabejotinas, kiti langeliai palikti tušti. Skyriaus pabaigoje pateikiami esminiai pastebėjimai ir rekomendacijos.

Remiantis dokumentų analize, Kinijos atvejis valstybės veiklos diapazone + ženklu "pagalbos" ir "diplomatijos" skiltyse nežymimas:

"**Valstybė draudžia kibernetines atakas" –** net pats autorius yra pastebėjęs, kad valstybės negali nuolat pilnai užtikrinti visiškos tūkstančių kompiuterių veiklos jos teritorijoje.[116]

"Valstybės draudžia, bet ne pakankamai"- šią kategoriją atitinka valstybės, kurios siekia kooperuotis norėdamos sustabdyti iš trečiųjų šalių kylančias atakas, tačiau dėl teisinės sistemos spragų, procedūrų, techninių pajėgumų ar politinės valios stokos nėra pajėgios to padaryti. Taip pat ją atitiktų nukentėjusi valstybė, kuri neša pasyvią atsakomybę dėl atakos, negalėdama jos sustabdyti, ir turėdama nesaugias sistemas. Pateikti pavyzdžiai rodo, kad Kinija yra viena iš pajėgiausių valstybių kibernetikos srityje, neabejojama, turėdama tokius techninius pajėgumus, patirtį ir žinias, ji galėtų sustabdyti atakas arba bent jau taikyti konkrečias draudžiančiąsias priemones. Interneto apribojimas nėra pakankama sąlyga laikyti, kad valstybė kibernetines atakas draudžia interneto filtravimu, priešingai, stabdomas

[115] Ten pat.
[116] Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks". Atlantic Council, US, 2011, 2.

informacijos srautas vartotojams, todėl nei “pagalbos”, nei “diplomatijos” skiltis nėra žymima +. Nors minimalių bandymų rasti teisinį sutarimą tarp Kinijos ir Vakarų demokratijų būta, rasti bendro sutarimo nei dėl kibernetinių atakų traktavimo, nei dėl “suvereniteto kibernetinėje erdvėje” apibrėžimo nepavyko.

“**Valstybės vykdoma (tiesiogiai)”/ ”Valstybė įsitraukusi**” – į šią kategoriją patenka valstybės, kurių vyriausybės planuoja ataką, naudodamos kibernetines pajėgas, esančios jų žinioje arba valstybės vyriausybės atakuoja naudodamos integruotais trečiųjų šalių ir valstybiniais pajėgumais. Nors Kinijos vyriausybė oficialiais pranešimais neigia neteisėtą veiklą JAV kibernetinėje erdvėje ir kontratakuoja argumentu, jog būtent JAV yra atsakinga už daugumą Kinijos patiriamų atakų, tokia pozicija nėra pagrindžiama jokias viešai prieinamais tyrimų duomenimis. Kitą vertus šios dvi kategorijos spektre rodo stiprų valstybės įsitraukimą, norint neabejotinai pagrįsti tokius kaltinimus, nepakanka vien įvardyti programišių grupuotės sąsajų su Kinijos vyriausybe. Healey nedetalizuoja, kokiu atveju argumentai laikomi pakankamais, todėl hipotetiškai galima daryti prielaidą, kad stiprų valstybės įsitraukimą patvirtintų šio klausimo iškėlimas tarptautinių organizacijų lygmeniu, siekiant sustabdyti programiščių veiklą ir pradėti teisinį procesą prieš Kinijos vyriausybę, kaip pažeidžiančią eilę teisinių dokumentų.

Kinijos atveju, dėl interneto kontrolės, sunku nustatyti skirtį tarp valstybės skatinamų, koordinuojamų ir užsakomų veiksmų. Remiantis žiniomis apie Kinijos pajėgumus, galima daryti prielaidą, jog tokio masto kompleksiškos, pasikartojančios, aiškiai į JAV karybos sritį nukreiptos atakos taikant naujausias ir pažangiausias technologijas, negalėtų būti laikomos be valstybės žinios.

Remiantis dokumentų analize, atsižvelgiant į autoritarinę valdymo formą, valstybės pajėgumus ir mąstą, + ženklu “pagalbos” skiltyse žymima:

“Valstybė ignoruoja”- šią kategoriją spektre turi valstybė, kurios vyriausybė turi žinių apie trečiosios šalies atakas, bet nenori imtis jokių oficialių veiksmų. Kinijos vystomi pajėgumai, jų panaudojimas prieš JAV tinklus leidžia manyti, kad vyriausybei yra patogu nesikišti į programišių veiklą, taip pat patogi situacija dėl teisinio reglamentavimo – JT Generalinėje Asamblėjoje Kinijos ir partnerių pasiūlymai atmesti, kaip nepriimtini tarptautinei bendruomenei, tuo tarpu Kinijai nepriimtini Budapešto Konvencijos punktai.

“Valstybė skatina”/ ”Valstybė formuoja”/ ”**Valstybė koordinuoja**”- remiantis Mandiant rezultatai ir Pentagono pranešimu, už kibernetines atakas atsakinga programišių grupuotė, operacijas vykdanti iš lokacijos, kur įsikūrusi slapta Kinijos karinė divizija (žinoma kaip Unit

61398). Valstybės skatinimu skalėje Healey siūlo laikyti, kai kibernetinės atakos panaudojamos kaip politikos priemonė, kai trečioji šalis planuoja ir vykdo atakas, o valstybės vyriausybė tokius veiksmus skatina. Valstybė nelinkusi bendradarbiauti tiriant atakas. Autoriaus apibūdinimas pilnai atitinka Kinijos atvejį. Neabejotina, kad Kiniją galima priskirti ir prie "valstybė formuoja" ir "valstybė koordinuoja" skilčių, kai trečioji šalis planuoja ir vykdo atakas, o valstybės vyriausybė jas dalinai remia; valstybės vyriausybė koordinuoja trečiosios šalies veiksmus, pvz. teikdama pasiūlymus jų įgyvendinimui (operaciniame lygmenyje). Atsižvelgiant į naudojamus pajėgumus, vargu ar bet kokia programišių grupuotė būtų pajėgi juos įsigyti be valstybės paramos.

Remiantis dokumentų analize, atsižvelgiant į autoritarinę valdymo formą, valstybės pajėgumus ir mąstą, + ženklu "pagalbos", tačiau - "diplomatijos" skiltyse, dėl bendrų sutarimų su tarptautine bendruomene atakų kibernetinėje erdvėje traktavime trūkumo, žymima:

"Valstybė užsako"- valstybės vyriausybė nukreipia trečiosios šalies veiksmus, taigi jie vykdomi jos vardu. Ši kategorija iš pirmo žvilgsnio atrodo kardinali, tačiau Healey išplėtojo idėją, teigdamas, kad į ją patenka valstybės, kurių nacionalinės vyriausybės, naudojasi trečiosios šalies vykdomomis atakomis, kaip politikos priemone. Ataka vykdoma valstybės, trečiosios šalies rankomis, programišiai, remiantis tarptautine teise, laikomi *de facto* valstybės agentais. Šiuo atveju, autorius pasiūlo į atakas žiūrėti per egzistuojantį teisinį precedentą "valstybė privalo nukreipti arba kontroliuoti – o ne tiesiog palaikyti, skatinti ar netgi toleruoti – privatų veikėją".[117] Atsižvelgiant į Kinijos valdymo formą ir griežtą privataus sektoriaus kontrolę, programišių veiksmai, nukreipti prieš JAV, atitinka šio spektro elemento keliamas sąlygas.

"Valstybės vykdoma užslėptai" – tai stipraus valstybės įsitraukimo kategorija, kuomet valstybė ne tik užsako, bet iš esmės ir įgyvendina atakas per slaptus subjektus, grupes, kurios yra tiesiogiai sukurtos ar kontroliuojamos valstybės. Trečioji šalis vykdo atakas, todėl valstybės vyriausybė gali neigti įsitraukimą planuojant ir įgyvendinant atakas. Apie Kinijos vykdomus slaptus įsibrovimus į JAV sistemas per kontroliuojamus subjektus patvirtina Mandiant nustatyta programišių grupė, veikianti Kinijos karinės divizijos lokacijoje ir taikanti naujausias kibernetines technologijas.

[117] Derek Jinks, "State Responsibility for the Acts of Private Armed Groups," *Chicago Journal of International Law, Vol. 4*, 2004. iš Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks".

Valstybės veiklos diapazonas		Pagalba	Diplomatija
	Valstybė draudžia kibernetines atakas		
	Valstybė draudžia, bet ne pakankamai		
	Valstybė ignoruoja	+	
	Valstybė skatina	+	
	Valstybė formuoja	+	
	Valstybė koordinuoja	+	
	Valstybė užsako	+	-
	Valstybės vykdoma užslėptai	+	-
	Valstybės vykdoma (tiesiogiai)		
	Valstybė įsitraukusi		

3.1. Pastebėjimai ir rekomendacijos:

J.Healey rekomendavo valstybės veiklos diapazono spektrą taikyti tiek siekiant apibūdinti individualias atakas, tiek atakų kampaniją. Kinijos ir JAV atveju, kaip autorius ir pastebėjo, Kinija atitinka keletą kriterijų. Visgi manyčiau, kad dokumentų analizė leidžia teigti, jog Kinijos atvejis labiausiai atitinka "Valstybė užsako" ir "Valstybės vykdoma užslėptai" kategorijas. Visi Kinijos veiklos kibernetinėje erdvėje pavyzdžiai leidžia kalbėti apie precedentą - Kinijos norą nelegaliu keliu rinkti informaciją apie JAV karinį pasirengimą, visais atvejais JAV aiškiai įvardijo kaltinimus Kinijai, remdamasi oficialiais ir viešai prieinamais dokumentais (privačios kibernetinio saugumo kompanijos Mandiant atliktu tyrimu ir Pentagono ataskaita, įvardijančia Kiniją kaip grėsmę). Kinija neigia bet kokius kaltinimus dėl neteisėtos veiklos kibernetinėje erdvėje, tačiau JAV turi duomenų apie ilgą laiką iš Kinijos teritorijos veikiančios programišių grupuotės veiklą. Atsižvelgiant į naująsias technologijas, kurios naudojamos siekiant išgauti slaptą JAV žvalgybos, diplomatinio korpuso, ekonomikos ir gynybos sektorių informaciją, vargu ar pavieniai programišiai galėtų tai pasiekti.

Bandant išskirti priežastis, kodėl JAV, net aiškiai įvardijusi Kiniją kalta dėl ilgalaikio kibernetinio šnipinėjimo, netaiko valstybės atsakomybės:

a) Pirmoji priežastis labai fundamentali – dvi didžiosios valstybės, turinčios vienus pajėgiausių pasaulyje ginkluočių sistemų (tiek kinetinių, tiek kibernetinių ginklų prasme), nenori eskaluoti konflikto, kuris vestų į karinius veiksmus. Nors vis dar diskutuojama, ar kibernetinė ataka gali sukelti karą, t.y. atsaką kinetine jėga, panašu, kad nei viena valstybė atsakymo rasti per praktiką nenori.
b) JAV, o kartu ir kitų Vakarų demokratijų, suvereniteto apibrėžimas (kas atsispindi ir teisinių dokumentų, taikytinų kibernetinių konfliktų atveju, analizėje) labai skiriasi nuo kiniškojo. Kinija linkusi į suverenitetą kibernetinėje erdvėje žiūrėti taip pat, kaip ir fiziniame pasaulyje, kibernetinis suverenitetas traktuojamas kaip teritorija tarp valstybių, kuriai taikoma vidaus teisė.
c) JAV ir Kinijos suvokimas, kaip suvereniteto kibernetinėje erdvėje principas turėtų būti taikomas valstybės piliečiams ir jos teritorijoje veikiančioms organizacijoms, ženkliai skiriasi. JAV pasisako už žodžio ir individo saviraiškos laisvės

užtikrinimą, tuo tarpu Kinijos vyriausybė sprendžia, kas interneto erdvėje yra netinkama.[118]

Nepaisant paprastos ir lengvai taikytinos J.Healey schemos, norint aiškiai ir nekvestionuojamai nustatyti, kuriai kategorijai priklauso valstybė, reikia didelio kiekio patikimų duomenų, kuo remiantis galima teigti apie valstybės įsitraukimą rengiant, koordinuojant ar vykdant kibernetines atakas. Nors Kinija yra viena didžiųjų valstybių, tačiau autoritarinis valdymas ir interneto kontrolė apsunkina šaltinių paiešką. Atliekant analizę remtasi tik antriniais šaltiniais, nepriklausomais spaudos pranešimais. Kad šis modelis būtų taikytinas analizuojant kibernetinius konfliktus, o atsakomybės valstybei prisikyrimas įsitvirtintų kaip praktika, reikalingas įdirbis. Nuolatinės ataskaitos (panašios į tai, ką rengia JAV vyriausybė), aptariant kibernetines grėsmes ir jų šaltinius, ne tik veiktų kaip prevencinė priemonė, bet ir padėtų tolimesniems tyrimų etapams. Viename iš savo darbų pats Jasonas Healey pateikė siūlymą, jog JAV vyriausybė turėtų skatinti žvalgybą periodiškai leisti ataskaitas, apie Kinijos vykdomą šnipinėjimą.[119]

[118]Kimberly Hsu ir Craig Murray, "China and International Law in Cyberspace". U.S. – China Economic and Security Review Commision Staff Report, 2014, 4.

[119]Jason Healey, "How the U.S. Should Respond to Chinese Cyberespionage," New Atlanticist Policy and Analysis Blog, Atlantic Council, February 25, 2013. <http://www.acus.org/new_atlanticist/how-us-should-respond-chinese- cyberespionage.>

Išvados

Penktosios erdvės - kompiuterių tinklų ir sistemų panaudojimas - pastaruosius du dešimtmečius ženkliai išaugo, naujosios technologijos integruojamos šalia tradicinių oro, jūrų ir sausumos pajėgų. Skaičiuojama, kad kasdien valstybės patiria tūkstančius kibernetinių atakų dėl įvairiausių techninių ir politinių priežasčių: siekiant šnipinėti ir pasisavinti informaciją, tobulinti savo sistemas, skleisti propagandą, sukelti laikinus sistemos sutrikimus ar sistemas išjungti. Kibernetikos specifika, t.y. anonimiškumas ir realios teisinės atsakomybės išvengiamumas, daro valstybių kibernetinę erdvę dar patrauklesne.

Pripažįstama, kad atsakomybės už neteisėtus veiksmus priskyrimas valstybei yra vienas esminių tarptautinio saugumo užtikrinimo elementų. Ilgą laiką manyta, kad kibernetinėje erdvėje vykstančių incidentų priskyrimas valstybių atsakomybei nėra įmanomas dėl pernelyg sudėtingo techninio proceso bei neaiškumo, kuo remiantis galima priskirti atakas valstybei, kai jos vykdomos nevyriausybinių veikėjų.

Tačiau pastarojo dešimtmečio tendencijos kinta. Analizuojant kibernetikos srities ekspertų darbus pastebėta, kad atliekant kibernetinių konfliktų analizę vis dažniau remiamasi prielaida, jog nacionalinės valstybės, o ne individai turi būti laikomi atsakingais už veiksmus kibernetinėje erdvėje, kenkiančius kitai valstybei ar jos sistemoms. Lyginat tarptautinius dokumentus, apibrėžiančius teises ir pareigas kibernetinėje erdvėje, ryškėja tendencija laikytis Jasono Healey pasiūlyto atsakomybės priskyrimo apibrėžimo, pagal kurį "valstybės neša atsakomybę už pagrindines atakas, kylančias iš valstybės teritorijos ar piliečių"[120]. Ši "iš viršaus į apačią" perspektyva, apimanti ir nevyriausybiniu veikėjus, veikiančius valstybės teritorijoje ar su valstybės žinia, atsispindi autoriaus pateiktame valstybės įsitraukimo į atakas spektre, kuris taikytas atvejo analizei.

Darbe išsikeltas tikslas, remiantis egzistuojančiomis atsakomybės už kibernetinius išpuolius teorinėmis prielaidomis bei praktiniais precedentais nustatyti sąlygas ir aplinkybes, kada valstybė tampa atsakinga už įvykdytas kibernetines atakas bei įvertinti, ar egzistuojančios tarptautinės teisės normos yra pakankamos numatyti valstybių atsakomybę kibernetinių konfliktų atvejais. Pateikiamas teorinis modelis, patobulintas atsižvelgiant į tyrimo problemą bei teorinės prielaidos, leidžiančios teigti, jog valstybė atitinka vieną ar kitą kategoriją. Chronologiška tvarka pateikiami teisiniai dokumentai, kurie apibrėžia kibernetinę

[120] Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks". Atlantic Council, US, 2011, 1.

erdvę tarptautiniu lygiu. Ši analizė leido pastebėti, kaip kito susidomėjimas kibernetinės erdvės problema[121], priežastis, kodėl atsakomybės priskyrimas nėra sėkmingas ir daryti bendresnius pastebėjimus: egzistuojančių tarptautinės teisės normų numatant valstybių atsakomybę kibernetinių konfliktų atveju pakankamumą bei kokios sąlygos ir aplinkybės būtinos, kad valstybė taptų atsakinga už įvykdytas kibernetines atakas. Grėsmėms kibernetinėje erdvėje kintant, dažnėjant ir modernėjant technologijai, būta poreikio pritaikyti tarptautinę teisę nagrinėti valstybės atsakomybę už neteisėtus veiksmus kibernetinėje erdvėje. Iš lėto, tačiau užtikrintai siekiama tarptautinės bendruomenės sutarimo dėl kibernetinės erdvės suvereniteto apibrėžimo, bendrų standartų ir normų dėl neteisėtų veiksmus prieš kitos valstybės kibernetinę erdvę traktavimo. Šias pastangas vainikuoja 2017 m. Talino Vadovo 2.0, orientuoto į kibernetines operacijas prieš kitas valstybes, parengimas, todėl reiktų sutikti, kad teisinė bazė nuolat atnaujinama, papildoma, kinta, atsižvelgiant į naujai iškylančias grėsmes ir augantį poreikį į jas reaguoti. Visgi esmine problema išlieka valstybių vyriausybių politinė valia, kaip būtina sąlyga, sėkmingai priskirti atsakomybę. Valstybių pastangos iškelti atsakomybės priskyrimo klausimą į tarptautinių organizacijų lygmenį ir siekis analizuoti kiekvieną atvejį bei sukurti precedentą, jog neteisėta veikla prieš kitas valstybes kibernetinėje erdvėja nėra toleruojama, yra būtini elementai, siekiant valstybės atsakomybės užtikrinimo.

Garsiai eskaluojamų ir konkrečioms valstybės priskiriamų atakų kibernetinėje erdvėje pavyzdžių rasti nesunku, tačiau įdomu pasižiūrėti didžiųjų valstybių reakcijas į kibernetinių atakų virtinę. Atvejo studijai pasirinktas 2013 m. Pentagono metiniame pranešime aiškiai įvardytas Kinijos šnipinėjimas, trukęs daugiau nei septynerius metus. Kinijos vyriausybė kaltinimus neigė, tuo tarpu JAV privati saugumo kompanija pateikė duomenis, neabejotinai liudijančius apie šalies indėlį kibernetiniam šnipinėjimui prieš JAV karinį ir gynybos sektorių. Duomenų paieška iš JAV pusės analizei lengvai prieinama, tiek Pentagono pranešimas, tiek, privačios saugumo kompanijos Mandiant atliktas tyrimas viešai pateiktas vartotojams. Kinijos vyriausybė vykdo griežtą interneto filtravimą, nedidelė dalis viešų valdžios atstovų pranešimų prieinamų tarptautiniai auditoriai, juose trūksta įrodymais paremtų faktų, kas leidžia abejoti informacijos patikimumu. Esant galimybei, būtų įdomu atlikti analizę, remiantis duomenimis iš abiejų valstybių vyriausybių, nes Kinija kontratakuoja kaltinimais dėl neteisiškos JAV veiklos kibernetinėje erdvėje. Nepaisant gana

[121] Vieni linksta manyti, kad kibernetinėmis grėsmėmis susidomėta po Estijos kibernetinės atakos 2006 m., kiti kibernetines grėsmes įtraukia į netradicinių grėsmių sąrašą, įvesdami sąvoką "kibernetinis terorizmas" ir jo pradžia laikydami 9/11 įvykius 2001 m. JAV.

vienašališkai pateiktos informacijos, JAV vyriausybės argumentai, grįsti įrodymais, skatino pabandyti pritaikyti J. Healey siūlomą valstybės atsakomybės priskyrimo spektrą.

Remiantis turimų duomenų analize, Kinija atitinka dvi pozicijas spektre: "valstybė užsako" ir "valstybės vykdoma užslėptai". Abi spektro kategorijos suponuoja apie stiprų valstybės įsitraukimą planuojant, organizuojant ir vykdant kibernetines atakas prieš JAV informacinius tinklus. Atakos vykdomos valstybės, trečiosios šalies rankomis (programišių grupuotė, veikianti netoli Šanchajaus, kur įsikūrusi slapta Kinijos karinė divizija (žinoma kaip Unit 61398), programišiai, remiantis tarptautine teise, laikomi *de facto* valstybės agentais. Trečioji šalis vykdo atakas, todėl valstybės vyriausybė gali neigti įsitraukimą planuojant ir įgyvendinant atakas. Atlikus tyrimą paaiškėjo galimos priežastys, kodėl JAV įvardijus Kiniją kalta dėl ilgalaikio šnipinėjimo, valstybės atsakomybė už atakas netaikoma. Pirmiausiai, tai didžiųjų valstybių nenoras eskaluoti konflikto, kuris galimai vestų į karinius veiksmus. Antra, valstybių suvokimas apie žmogaus teisę bei tarptautinę sistemą apskritai ženkliai skiriasi, taip pat nesutariama ir dėl esminių sąvokų, tokių kaip "kibernetinis suverenitetas". Esant šioms sąlygoms, valstybės atsakomybės Kinijai taikymas yra itin komplikuotas, todėl nenuostabu, kad netgi remiantis egzituojančią teisine baze, JAV artimiausiu metu nesiims akivaizdžių veiksmų.

Nepaisant to, jog J.Healey atsakomybės priskyrimo valstybei spektras yra paprastas ir universaliai pritaikomas, jame pateiktos kategorijos tarpusavyje glaudžiai siejasi, todėl sudėtinga argumentuotai priskirti valstybę vienai kategorijai atmetant kitą. Nors autorius pabrėžia, kad valstybė gali vienu metu atitikti kelias spektro kategorijas, tačiau lieka neaišku, kuo galutiniame procese skirsis valstybės atsakomybė, priklausomai nuo pozicijos spektre. Jeigu įmanoma, jog valstybė vienu metu atitinka kelias pozicija, tuomet ar galima teigti, kad valstybei, kuri patenka į kelias stipraus valstybės įsitraukimo kategorijas, bus taikoma griežtesnė atsakomybė už atakas, nei tai, kuri patenka tik į vieną sunkios atsakomybės ar kelias mažesnio įsitraukimo kategorijas spektre. Šių atsakymų autorius nepateikė nei viename darbe, tačiau tikėtina, kad ši spraga paliekama tikslingai, nustačius valstybės įsitraukimą ir priskyrus atsakomybę valstybei, pats atsakomybės įgyvendinimas paliekamas spręsti teisės įgyvendinimo institucijoms. Visgi būtų įdomu susipažinti su išbaigta metodologija, kurioje atsispindėtų, kaip taikant spektrą ir priskyrus atsakomybę valstybei, imamasi teisės įgyvendinimo, priklausomai nuo valstybės įsitraukimo organizuojant, remiant ar vykdant kibernetines atakas.

Literatūros sąrašas:

1. Arimatsu, L., "A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations". 4th International Conference on Cyber Conflict Proceedings, supra note 6, 2012.

2. Berger, Peter L. ir Thomas Luckmann, *The Social Costruction of Reality*. Penguine Books, 1966.< http://perflensburg.se/Berger%20social-construction-of-reality.pdf>
3. Cavelty, Myriam Dunn, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. London: Routledge, 2008.
4. CCDCOE, "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", NATO Cooperative Cyber Defence Centre of Excellence, Estonia, 2017. <https://ccdcoe.org/sites/default/files/documents/CCDCOE_Tallinn_Manual_Onepager_web.pdf>
5. Council for Security Cooperation in the Asia Pacific (CSCAP), "Ensuring A Safer Cyber Security Environment", Memo. No. 20, 2012. <http://www.cscap.org/uploads/docs/Memorandums/CSCAP%20Memorandum%20No%202%20--%20Asia%20Pacific%20Confidence%20and%20Security%20Building%20Measures.pdf>
6. Council of Europe, "Convention on Cybercrime", 2001. < https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561>
7. Cyber Attacks From China Are Bleeding the U.S., Center of Security Policy, 2016. <https://www.centerforsecuritypolicy.org/2016/05/17/cyber-attacks-from-china-are-bleeding-the-u-s/>

8. Davidson, Jacob, "China Accuses U.S. of Hypocrisy on Cyberattacks". Time, 2013. <http://world.time.com/2013/07/01/china-accuses-u-s-of-hypocrisy-on-cyberattacks/>
9. Draft Article on Responsibility of States for Internationally Wrongful Acts, 2001. <http://untreaty.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf>
10. European Commission, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", 2013. < http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf >
11. European Network and Information Security Agency (ENISA), "National Cyber Security Strategies: Practical Guide on Development and Execution", 2012. <http://www.enisa.europa.eu/activities/ Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security- strategies-an-implementation-guide>
12. FireEye, "Threat Intelligence Report", <https://www.fireeye.com/current-threats/threat-intelligence-reports.html>,
13. Greenemeier, Larry, "China's Cyber Attacks Signal New Battelfield Is Online", Scientific American, 2007. <https://www.scientificamerican.com/article/chinas-cyber-attacks-sign/>

14. Healey, Jason, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks". Atlantic Council, US, 2011.
15. Healey, Jason, "How the U.S. Should Respond to Chinese Cyberespionage," New Atlanticist Policy and Analysis Blog, Atlantic Council, February 25, 2013.

<http://www.acus.org/new_atlanticist/how-us-should-respond-chinese-cyberespionage.>
16. Hsu, Kimberly ir Craig Murray, "China and International Law in Cyberspace". U.S. – China Economic and Security Review Commission Staff Report, 2014. <https://www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf>
17. Hunter, D., "Cyberspace as Place and the Tragedy of the Digital Anticommons", California Law Review: 91, 2003.
18. Internet Users, Internet Live Stats <http://www.internetlivestats.com/internet-users/>
19. Lessig, L., "The Law of the Horse: What Cyberspace Might Teach*",* Harvard Law Review:113, 1999.
20. Lewis, James A, "The "Korean" Cyber Attacks and Their Implications on Cyber Conflict". Center of Strategic and International Studies, 2009. <https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf>
21. Leyden, John, "France blames China for hack attack". The Register, 2007. <https://www.theregister.co.uk/2007/09/12/french_cyberattacks/>
22. Marcus, Jonathan, "US accuses China government and military of cyber-spying". BBC News, 2013. <http://www.bbc.com/news/world-asia-china-22430224>
23. McKune, Sarah, "An Analysis of the International Code of Conduct for Information Security", 2015. <https://citizenlab.org/2015/09/international-code-of-conduct/>
24. Melzer, Nils, "Cyberwarfare and International Law", UNIDIR, 2011. <http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf>
25. Ministry of Foreign Affairs of the People's Republic of China, Address by Vice Foreign Minister Li Baodong at the Opening Ceremony of the International Workshop on Information and Cyber Security, 2014 m. birželio 5 d. <thttp://www.fmprc.gov.cn /mfa_eng/wjbxw/t1162458.shtml>
26. Nakashima, Ellen, "Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies". The Washington Post, 2013. <https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html?utm_term=.5c8984050e80>
27. National Exposure Index, <https://information.rapid7.com/national-exposure-index.html>
28. Organization for Security and Co-operation in Europe, "The Astana Commemorative Declaration: Towards a Security Community", sum.doc./1/10//Corr.1, 2010 m. gruodžio 3 d. <http://www.osce.org/cio/74985?download=true>
29. Organization of American States, Secretariat of Legal Affairs, "Inter-American Cooperation Portal on Cyber-Crime". <http://www.oas.org/juridico/english/cyber.htm>
30. Paganini, Pierluigi, "NATO presents the Tallinn Manual 2.0 on International Law Applicable to cyberspace. Security Affairs, 2017. <http://securityaffairs.co/wordpress/56004/cyber-warfare-2/nato-tallinn-manual-2-0.html>

31. Perlroth, Nicole, “Hackers in China Attacked The Times for Last 4 Months”. The New York Times, 2013. <http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html>
32. Prosecutor v. Dusko Tadic, “Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction”, IT- 94-1-A, 1995. < http://www.refworld.org/cases,ICTY,47fdfb520.html>
33. Rid, Thomas ir Ben Buchanan, “Attributing Cyber Attacks”, Journal of Strategic Studies, 38:1-2, 2015.
34. Riley, Charles, “Report: Chinese military engaged in “extensive cyber espionage campaign”. CNN, 2013. <http://money.cnn.com/2013/02/19/technology/china-military-cybercrime/index.html?iid=EL>
35. Rosenzweig, Paul, “Significant Cyber Attacks on Federal Systems – 2004-present”, Lawfare, 2012. <https://www.lawfareblog.com/significant-cyber-attacks-federal-systems-2004-present>
36. Ryan, J., “Countering Militant Islamist Radicalisation on the Internet: A User Driven Strategy to Recover the Web”. Dublin: IIEA, 2007.
37. Sanger, David E., “U.S. Blames China’s Military Directly for Cyberattacks”. The New York Times, 2013. <http://www.nytimes.com/2013/05/07/world/asia/us-accuses-chinas-military-in-cyberattacks.html>
38. Sarah McKune, “An Analysis of the International Code of Conduct for Information Security”, 2015. <https://citizenlab.org/2015/09/international-code-of-conduct/>
39. Schmitt, M. N., “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework”, Columbia Journal of Transnational Law:7, 1998.
40. Segal, Adam, “Shaming Chinese hackers won’t work because cyber-espionage is here to stay. The Guardian, 2013. <https://www.theguardian.com/commentisfree/2013/may/30/china-hacking-cyber-espionage-obama>
41. Shackelford, Scott J. ir Richard B.Andres, “State Responsibility for Cyber Attacks: Competing Standarts for a Growing Problem”. Georgetown Journal of International Law, Vol.42, 2011.
42. Shackelford, Scott J., “State Responsibility for Cyber Attacks: Competing standards for a growing problem”. Conference on Cyber Conflict, Estonia, 2010.
43. Sklerov, Matthew J., “Solving the Dilemma of States Responses to Cyberattacks: a Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent”, 2009. <https://www.hsdl.org/?view&did=12115>
44. Swaine, Michael D., “Chinese Views on Cybersecurity in Foreign Relations”. China Leadership Monitor, no. 42. <http://www.hoover.org/sites/default/files/uploads/documents/CLM42MS.pdf>
45. Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013. <http://csef.ru/media/articles/3990/3990.pdf>
46. The Cyberterrorism Project, 2010. <http://www.cyberterrorism-project.org/cyberterrorism-report/>
47. Titcomb, James, “Mapped: The countries most vulnerable to cyber-attacks”, The Telegraph, 2016. <http://www.telegraph.co.uk/technology/2016/06/10/mapped-the-countries-most-vulnerable-to-cyber-attacks/>
48. Top 10 Countries Where Cyber Attacks Originate, Government Technology, 2013. <http://www.govtech.com/security/204318661.html>;

49. Top 10 Countries with Most Hackers in the World, Cyware, 2016. <https://cyware.com/news/top-10-countries-with-most-hackers-in-the-world-42e1c94e>
50. Top 20 Countries Found to Have the most Cybercrime <https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/>
51. Tosh, Caroline, "Genocide Acquittal Provokes Legal Debate", Institute of War and Peace Reporting, 2007. < https://iwpr.net/global-voices/genocide-acquittal-provokes-legal-debate>
52. Townsend, Kevin, "NATO Published Tallinn Manual 2.0 on International Law Applicable to Cyber Ops". Security Week, 2017. <http://www.securityweek.com/nato-publishes-tallinn-manual-20-international-law-applicable-cyber-ops>
53. U.N.G.A., Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security, 2013.
54. U.S. House Energy and Commerce Committee, "Hearing on Cyber Espionage and the Theft of U.S. Intellectual Property and Technology", testimony of James Lewis, 2013 birželio 9 d.
55. United Nations General Assembly, A/66/150, 2011. <https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf>
56. United Nations General Assembly, A/69/723, 2015. <https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf>
57. Vadapalas, Vilenas, "Tarptautinė teisė. Pagrindiniai dokumentai ir jurisprudencija". Vilnius, Eugrimas, 2003.
58. Verton, D., *Black Ice: The Invisible Threat of Cyberterrorism*. Cambridge: CUP., 2003.
59. Wan, William ir Ellen Nakashima, "Report ties cyberattacks on U.S. computers to Chinese military". The Washington Post, 2013. <https://www.washingtonpost.com/world/report-ties-100-plus-cyber-attacks-on-us-computers-to-chinese-military/2013/02/19/2700228e-7a6a-11e2-9a75-dab0201670da_story.html?utm_term=.7ca5d99a0a25>
60. Wolter, Detlev, "The UN Takes a Big Step Forward on Cybersecurity". Arms Control Association, 2013. <https://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity>
61. Yannakogeorgos, Panayotis A., "Strategies for Resolving the Cyber Attribution Challenge". Air Force Research Institute Papers, 2013.
62. Žilinskas, Justinas, "Kibernetinių technologijų panaudojimo ginkluotose konfliktuose poveikis tarptautinei humanitarinei teisei". Jurisprudencija, 20(3), 2013. <https://www.mruni.eu/upload/iblock/85d/JUR-13-20-3-17.pdf>

Summary

States' Attribution in Cyber Conflict: From Theoretical Approach to Common Practise

Development in information technologies led to a new type of threat in the field of international relations. Cyber attacks are already considered a threat to international stability, peace and security. For more than two decades, regardless of the efforts to attribute cyber attacks to particular states, there is no practise on how to hold incriminated states accountable. Previous attempts to attribute cyber attacks to specific states failed due to lack of technical proof. The global national security community needs to shift resources from the technical attribution towards solving the responsibility attribution problem.

While cyberspace is accessible to governments, non-state organizations, private enterprises and individuals it is easy to disguise the origin of an operation. However, reliable identification and attribution of cyber activities is particularly difficult. Internet enables anonymity more than security. Therefore, this bottom-up process of tracking particular actors instead of host countries is rarely successful. Recently, the discussions regarding cyber attribution took a new approach to the problem. Jason Healey shared the idea to look into cyber attribution as a top-down policy issue with nations held responsible for major attacks originating from their territory or conducted by their citizens. For national security policymakers, he says, knowing "who is to blame?" can be more important than "who did it?".[122]

Considering this approach, the problem question of this paper appears - although cyber attacks are becoming an increasing problem of national security, the state is not able to find appropriate mechanisms to define responsibilities for the attacks even if failure of responsibility attribution may minimize the efficiency to respond to cyber threats. The main objective remains to determine the conditions and circumstances in which the state is responsible for the committed cyber attack and to assess whether the existing rules of international law are sufficient to provide the framework for the responsibility fixation.

"Top-down" approach proposes a spectrum of state responsibility which helps to assign responsibility for a particular attack or campaign of attacks to the particular state. This spectrum, developed by J. Healey, allocates a different degree of responsibility, based on whether attacks ignored, encouraged, supported or conducted by national governments. In

[122] Jason Healey, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks". Atlantic Council, US, 2011, 1.

order to confirm this, paper introduces a case study for previously completed cyber attacks. The government and military of China was accused by US for cyber-spying between 2006 and 2013. A report by a private security firm tied cyber attacks on US computers to Chinese military. By using states responsibilities spectrum China falls into two categories: "state-ordered" and "state-rogue-conducted" according to these analyses. However, there are several reasons why the national responsibility of attacks in cyberspace at US – China case was not allocated. Firstly, regardless continuous cyber attacks, none of the countries desired to start the escalation which could lead to an armed conflict with a possible use of kinetic power. Secondly, US, as well as the other Western countries, and China share a completely different view on sovereignty over cyberspace. Finally, cooperation is the key in order to reduce the number of cyber attacks. China strongly disagrees with most of the documents proposed to attribute national responsibility for any attacks in cyberspace.

Cyberspace will remain insecure until nations will become more responsible for the actions they take in cyberspace, directly or indirectly, by using "third party" actors to mislead the international community. As the problem is growing, the resolution in regards to responsibility attribution is required. International law is becoming more and more adapted to consider illegal actions in cyberspace as any other illegal actions done by kinetic power. It is hopefully a near future scenario where the states' attribution in cyber conflict will become a reality.